T.C.
RECEP TAYYİP ERDOĞAN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

CEBİRSEL KRİPTOLOJİ YÖNTEMLERİ ve BAZI UYGULAMALARI

ENGİN YEŞİLBAŞ

TEZ DANIŞMANI
YRD. DOÇ. DR. ÜMİT DENİZ
TEZ JÜRİLERİ
DOÇ. DR. BAHADIR ÖZGÜR GÜLER
YRD. DOÇ. DR. YAVUZ KESİCİOĞLU

YÜKSEK LİSANS TEZİ
MATEMATİK ANA BİLİM DALI

RİZE-2016

T.C.

RECEP TAYYİP ERDOĞAN ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

CEBİRSEL KRİPTOLOJİ YÖNTEMLERİ ve BAZI UYGULAMALARI

Yrd. Doç. Dr. Ümit DENİZ danışmanlığında, **Engin YEŞİLBAŞ** tarafından hazırlanan bu çalışma, Enstitü Yönetim Kurulu kararıyla oluşturulan jüri tarafından 26./07/2016 tarihinde MATEMATİK Anabilim Dalı'nda **YÜKSEK LİSANS** tezi olarak kabul edilmiştir.

Jüri Üyeleri	**Ünvanı Adı ve Soyadı**	**İmzası**
Başkan :	Yrd. Doç. Dr. Ümit DENİZ	
Üye :	Doç. Dr. Bahadır Özgür GÜLER	
Üye :	Yrd. Doç. Dr. Yavuz KESİCİOĞLU	

Prof. Dr. Selami ŞAŞMAZ

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRÜ

ÖNSÖZ

Cebirsel kriptoloji yöntemleri ve bazı uygulamalarının araştırıldığı bu çalışma süresi boyunca ilgi ve desteğini hiçbir zaman esirgemeyen çok değerli danışman hocam sayın Yrd. Doç. Dr. Ümit DENİZ'e teşekkürlerimi bir borç bilirim.

Çalışmalarım sırasında bana her türlü desteği veren Merkezi Satınalma Birimindeki değerli mesai arkadaşlarım Osman ŞİŞMAN, Eyüp GÜR, Fatih TURAN, Çetin BAYRAKTAR, Can KOSANOĞLU ve Mali Hizmetler Başkanımız Musa KORKUT'a tüm kalbimle teşekkür ederim.

Hayatımın her aşamasında bana maddi manevi her türlü desteği sağlayan, her zaman yanımda olan canım ailem; rahmetli babam Hüseyin, annem Ayşe, abim Önder, yengem Nurcan YEŞİLBAŞ ile ablam Nimet YILMAZ'a tüm kalbimle teşekkür ederim.

Engin YEŞİLBAŞ

TEZ ETİK BEYANNAMESİ

Tarafımdan hazırlanan "Cebirsel Kriptoloji Yöntemleri ve Bazı Uygulamaları" başlıklı bu tezin, Yükseköğretim Kurulu Bilimsel Araştırma ve Yayın Etiği Yönergesindeki hususlara uygun olarak hazırladığımı ve aksinin ortaya çıkması durumunda her türlü yasal işlemi kabul ettiğimi beyan ederim. 29/06/2016

Engin YEŞİLBAŞ

Uyarı: *Bu tezde kullanılan özgün ve/veya başka kaynaklardan sunulan içeriğin kaynak olarak kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanundaki hükümlere tabidir.*

ÖZET

CEBİRSEL KRİPTOLOJİ YÖNTEMLERİ ve BAZI UYGULAMALARI

Engin YEŞİLBAŞ

Recep Tayyip Erdoğan Üniversitesi
Fen Bilimleri Enstitüsü
Matematik Anabilim Dalı
Yüksek Lisans Tezi
Danışmanı: Yrd. Doç. Dr. Ümit DENİZ

Bu çalışmada, şifreleme biliminin ilk ortaya çıkışından günümüze kadar ki gelişimi hakkında bilgi sahibi olmak, geçmişte ve günümüzde kullanılan şifreleme yöntemleri ve algoritmalarının işleyişleri incelenmesi planlanmıştır. Temelde iki ana bölümden oluşan bu tezde, ilk bölümde kriptolojiye giriş, tarih boyunca kullanılan şifreleme yöntemleri ve ülkemizdeki kriptolojik çalışmalara yer verildi, kriptolojide kullanılan temel tanımlar ve kriptolojik işlemlerde kullanılan matematiksel tanım ve teoremler gösterildi. İkinci bölümde ise kriptografi ve kriptoanaliz tanımları yapıldı ve kriptografi yöntemleri olan Sezar şifreleme, yer değiştirme şifresi, Polybius dama tahtası, Bifid ve Trifid şifreleme, Playfair şifreleme, Affine şifreleme, Mors alfabesi, ADFGVX şifreleme, Vernam şifreleme, Vigenere şifreleme, Hill şifreleme, Kuvvet fonksiyonları ile şifreleme ve RSA şifreleme yöntemi sistemleri örneklerle birlikte incelendi.

2016, 67 sayfa

Anahtar kelimeler: Kriptoloji, Kriptografi, Şifreleme, Simetrik Şifreleme Yöntemleri, Asimetrik Şifreleme Yöntemleri.

ABSTRACT

ALGEBRAIC CRYPTOLOGY METHODS and SOME APPLICATIONS

Engin YEŞİLBAŞ

Recep Tayyip Erdoğan University
Graduate School of Natural and Applied Sciences
Department of Mathematics
Master Thesis
Supervisor: Asts. Prof. Dr. Ümit DENİZ

In this study, the aim is to examine and be informed about the development of the science of encryption since its first appearence; encryption methods and process of algorithms that have been used from past to present. This thesis consists of two parts: The first part includes cryptology input, the encryption method used throughout history and the cryptograhic studies that have been performed in our country, the basic definitions used in cryptography and mathematical theorems and definitions used in cryptographic operations have been demonstrated. In the second part, cryptography and cryptanalysis definitions have been given. Moreover; cryptography methods that are Caesar encryption, relocation password, Polybius checkerboard, Bifid and Trifid encryption, Playfair encryption, Affine encryption, Morse, ADFGVX encryption, Vernam encryption, Vigenere encryption, Hill encryption, encryption with power functions and RSA encryption systems have been examined along with examples.

2016, 67 pages

Keywords: Cryptology, Cryptography, Encryption, Symmetric Encryption Methods, Asymmetric Encryption Methods.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

SEMBOLLER ve KISALTMALAR DİZİNİ

$\varphi\ (m)$	Euler Phi Fonksiyonu
P	Açık Metin Uzayı
C	Şifreli Metin Uzayı
k	Şifreleme Anahtar Uzayı
e_k	Şifreleme Algoritması
d_k	Deşifreleme Algoritması
M.Ö	Milattan Önce
FEAL	Fast Data Encipherment Algorithm
SAFER	Secure and Fast Encryption Routine
DSA	Digital Signature Algorithm
NSA	National Security Agency
IBM	International Business Machines
RSA	Rivest Shamir Adleman
DES	Data Encryption Standart
IDEA	International Data Encryption Algorithm
PES	Packetized Elemantry Stream
PGP	Pretty Good Pivacy
SHA-1	Secure Hash Algorithm
NIST	National Institue of Standart and Technology
AES	Advanced Encryption Standart
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
EAÜ	Elektronik Araştırma Enstitüsü
TSK	Türk Silahlı Kuvvetleri
NATO	North Atlantic Treaty Organization
ABD	Amerika Birleşik Devletleri
MİLON	Milli Online Kripto Cihazı

1. GENEL BİLGİLER

1.1. Giriş

Ünlü düşünür Francis Bacon yüzyıllar önce ‘bilginin bir güç’ olduğunu ifade etmiştir. Bilgi, insanlar için her zaman kıymetli olmuştur ve çağlar boyunca toplumları etkilemiş, özellikle savaşları kazanmak, para kazanmak ve tarihi şekillendirmek için kullanılan önemli bir güç haline gelmiştir. Bazı bilgilerin hayati derecede önemli olmaya başlaması, onların gizli tutulması zorunluluğunu ortaya çıkarmıştır. Meraklı olan insanoğlu bu bilgilere ulaşmak istese de, geliştirilen çeşitli yöntemlerle bilgiyi çözülmesi güç bir gizem haline getirmeyi başarmıştır. Bunlardan biri olan kriptolojide bilgiyi yalnızca düşmandan gizlemek amacıyla kullanılmış olsa da günümüzde teknolojinin hayatımıza girmesiyle birlikte cep telefonlarından bankamatiklere, e-imzadan mail adreslerine kadar hayatımızın her anında yer alır vaziyete gelmiştir.

Kriptografi, Yunancada gizli-saklı anlamına gelen *kryptos* sözcüğü ile yazmak anlamına gelen *graphien* sözcüklerinden türetilmiştir. Kriptografi, gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür (Çimen vd., 2008). Kısaca, anlaşılır bir mesajı anlaşılmaz hale dönüştürme ve anlaşılmaz mesajı tekrar anlaşılır hale geri dönüştürme işlemidir (Şekil 1).

Şekil 1. Şifreleme akış şeması.

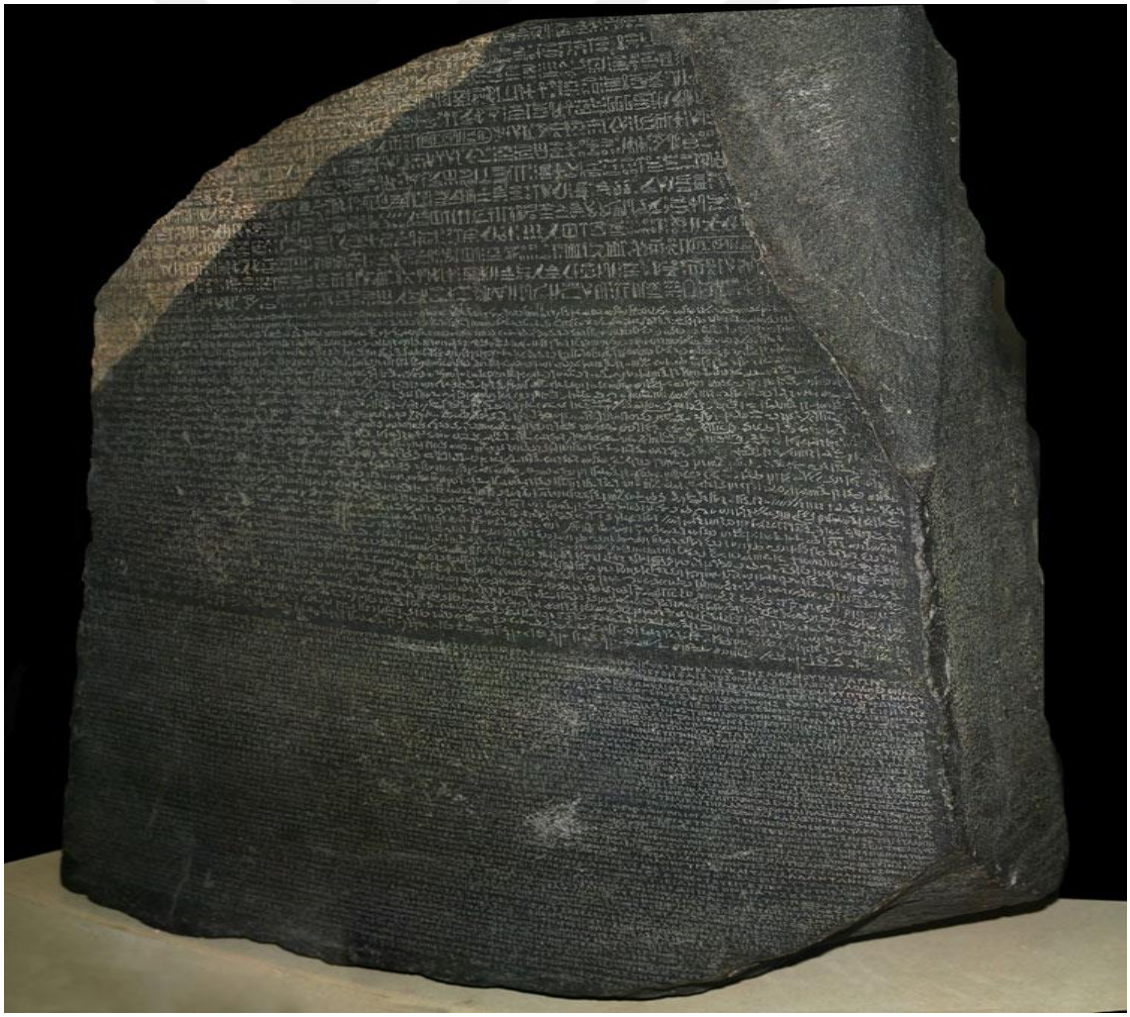
Kriptoloji ise; gizlilik, veri bütünlüğü, varlık doğrulanması, veri kaynağının doğrulanması gibi bilgi güvenliği ile ilgili konuları matematiksel teknikleri kullanarak çalışan bilim dalına denir (Menezes vd., 1997).

1.2. Kriptolojinin Tarihsel Gelişimi

Yazının icadını insanlık tarihinin başlangıcı olarak kabul edersek, yazıyla birlikte bilgi toplanabilir, saklanabilir ve iletilebilir bir hale gelmiştir. İnsanlar, belli süre sonra yazıyla haberleşmeye başlamış ancak; insanoğlunun karşı koyamadığı merakı yüzünden gönderilen mesajları gizleme yöntemine başvurmuşlardır.

İlk ortaya çıkışından itibaren çeşitli evreler geçirerek günümüze ulaşan kriptolojinin, tarihsel gelişimi kısaca şu şekildedir.

M.Ö. 1900: İlk kriptografik belge (Şekil 2), yaklaşık olarak M.Ö. 1900 yılında yazıldığı tahmin edilen Rosetta tabletidir (Khan, 1996).



Şekil 2. Rosetta tabletinin ön yüzü (URL-1).

M.Ö. 1500: Bir Mezopotamya tabletinde, çömleklerin cilalanması hakkında bilgilerin şifrelenmiş olarak bulunduğu anlaşılmıştır.

M.Ö. 600-500: Eski Ahit de (Hem Musevilerin hem Hristiyanların okuduğu kutsal kitap) yer alan ve Yeremya peygamberin (İbrani Peygamber) kehanet ve uyarılarında bazı şifrelere rastlanmıştır. Babil saldırısını önceden haber veren peygamber ATBASH (Alfabedeki, ilk harf son harfle, ikinci harf sondan ikinci harfle yer değiştirir) isimli bir şifre kullanmıştır (Khan, 1996).

M.Ö. 480: Herodotos'un yazdığına göre Pers Kralı Daryus'un elinde tutsak olan Yunanlı komutan Histiaeus, Anadolu'da Milet şehrinde ki damadı Aristagoras'a gizli bir mesaj göndermek istiyordu. Histiaeus, kölesinin saçını kazıtıp üzerine dövme yaptırmış, kölenin saçı uzayınca onu Milet'e göndermiş ve kölenin saçı kazıtılınca mesaj okunmuştur (Khan, 1996).

M.Ö. 60-50: Julius Caesar normal alfabedeki harflerin yerini değiştirerek oluşturduğu şifreleme yöntemini devlet haberleşmesinde kullandı. Bu yöntem açık metindeki her harfin alfabede kendisinden 3 harf sonraki harfle değiştirilmesine dayanıyordu (Khan, 1996).

M.Ö. 5: Yunanlılar tarafından kullanılan ve *Scytale* (Kalın bir sopaya, mesajın yazıldığı deri şerit sarılırdı. Mesaj şeridin üzerine sopa boyunca yazılır ve şerit açık olarak yollanırdı. Karşı taraf, şeridi aynı kalınlıkta bir sopaya sarıp mesajı okurdu.) adını verdikleri şifreleme cihazını kullanmışlardır (Şekil 3). Bu cihaz hem askeri amaçlı kullanılan hem de ilk kriptografik cihaz kabul edilmektedir (Khan, 1996).

Şekil 3. Scytale (URL-2).

600: Abdurrahman-El-Halil-İbn-i Ahmed'in yazdığı "Kitab'ül-Muamma" adlı kitapta, Bizans İmparatoru tarafından gönderilen Yunanca bir şifreli mektubun çözümü vardır (Çeşmeci, 2009).

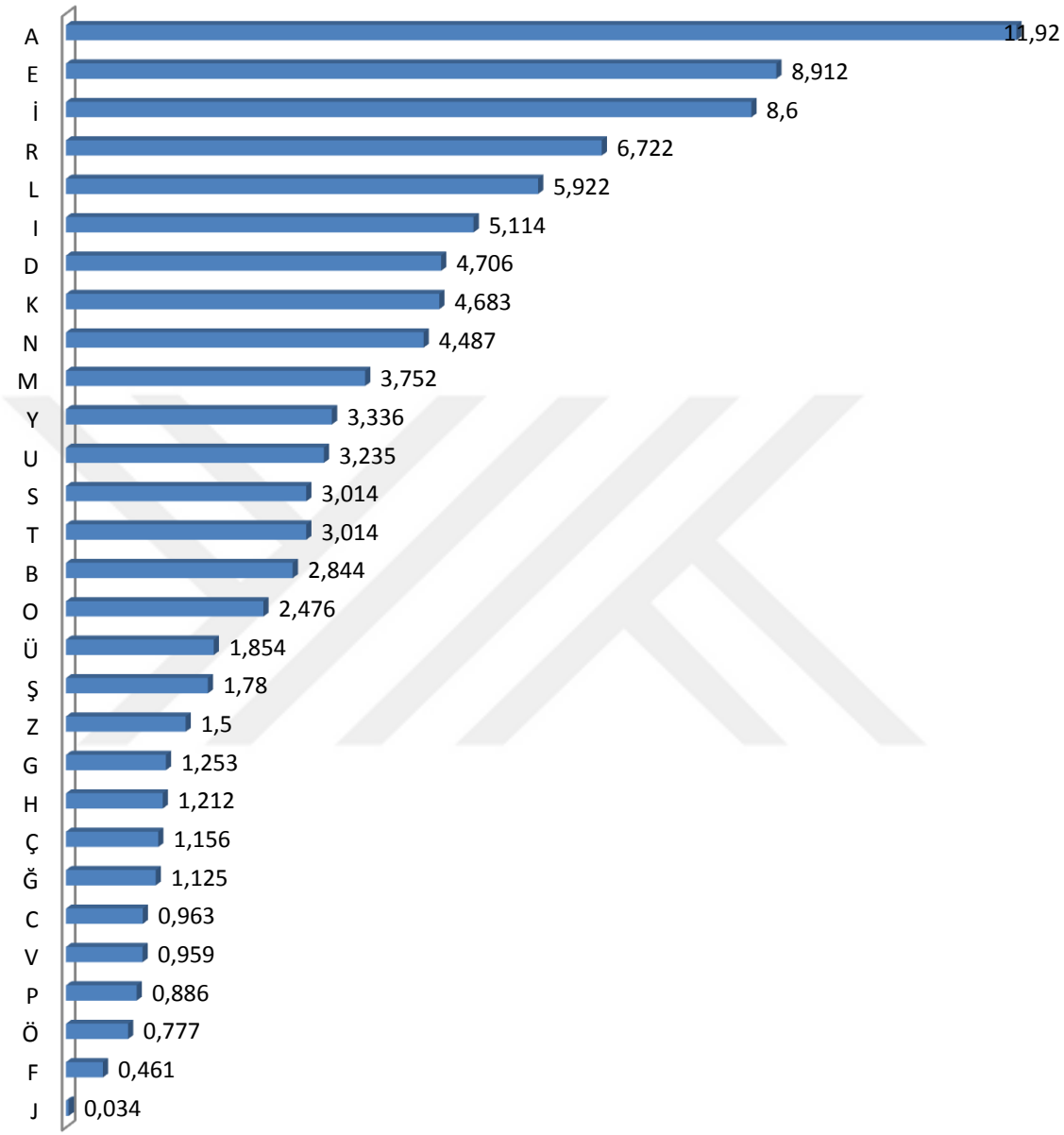
873: Arapların filozofu olarak bilinen Al-Kindi kriptanaliz üzerine yazılmış ilk makale olan *"Kriptografik Mesajların Deşifresi"* isimli makaleyi yazmıştır. Bu makale de frekans analizini ortaya atmıştır.

İstanbul Süleymaniye Osmanlı Arşivinde yer alan Al-Kindi'ye ait Kriptografik Mesajların Deşifresi isimli makalede frekans analizi kavramını ortaya atmıştır. Al-Kindi'ye göre yazıldığı dil bilinen şifreli bir mesajı çözmek için, aynı dilde yazılmış uzun bir metin bulup her harfin kullanım sıklığının hesaplaması yapılmalıdır. Metinde en sık kullanılan harf, şifreli mesajda en sık kullanılan harf demektir. Al-Kindi, bu yönteme frekans analizi adını vermiştir. Sebebi ise bir dildeki her harfin bir kullanım sıklığı, bir frekansı olması demektir.

Frekans analizi şifrelemeden ziyade bir kriptanaliz yöntemidir. Öncelikle şifrelenmiş metnin hangi dilde yazıldığını bilmek gerekir. Yazıldığı dil biliniyorsa, o dilin frekans analizini yapmak yeterli olacaktır. Şifre metinde en çok kullanılan harf, dilde en çok kullanılan harfe ya da harflerden birine denk gelecektir. Bu işlem en çok kullanılan harften en az kullanılan harfe doğru yapıldığında başarı oranı yüksektir (Çimen vd., 2008).

Türk alfabe sisteminde en çok kullanılan sesli harfler "A,İ,E" , en çok kullanılan sessiz harfler ise "N,R,L,K,D" harfleridir. En az kullanılan harfler ise "J,F,Ö,V,C" harfleridir (Tablo 1).

Tablo 1. Türkçe harflerin kullanım yüzdeliği (URL-3).



*Gazete köşe yazıları ve 9 yazara ait 37 kitaptan elde edilmiş, 11 milyon karakterden oluşan 13,4 MB boyutundaki metin seti üzerinden elde edilmiştir.

1300: İbn-u Haldun, maliyede ve orduda bazı yazıları gizlemek için şifrelerden faydalanmıştır.

1379: Gabriel Dilavandi, alfabelerin ve kodların yerini değiştirerek şifreler yazmış ve bu şifreler 400 yıl boyunca kullanılmıştır.

1412: Abdullah Kalkasadi'nin yazdığı 14 ciltlik *"Subhu'l Asa"* isimli ansiklopedi de şifrelemeye ait yöntemler vardır. Bu eserde kriptanalistin ilgilendiği dili bilmek zorunda olduğundan söz edilir ve Arapça 'da asla yan yana gelmeyen harflerin bir listesi vardır.

1450: Garip bitkiler, astronomik resimler ile resmedilen bir orta çağ el yazması olan Voynich Yazmalarının, 200 sayfalık kısmı bilinmeyen bir dilde yazılmış ve halen deşifre edilememiştir (Şekil 4).

Şekil 4. Voynich yazmalarından bir sayfa (URL-4).

1460: Leone Battista Alberti, Sezar şifrelerinin kullanımını basitleştiren eş merkezli iki diskten oluşan bir alet geliştirdi.

1518: Johannes Trithemus adında bir Alman rahip tarafından yazılan *"Polygraphie"* adlı kitapta çok alfabeli şifreleme sisteminden bahsedilmektedir.

1553: Giovan Batista Belaso adlı İtalyan bilim adamı daha sonra Vigenere Şifresine de ilham kaynağı olacak *"La Cifra Del Sig"* isimli kitabı yayınlamıştır.

1586: Fransız diplomat Blaise De Vigenere adına adanan Vigenere Şifresi, uzun yıllar boyunca *"le chiffre indechiffrable"* yani kırılamayan şifre olarak adlandırılmıştır. Uzun yıllar güvenirliliğini koruyan bu şifre 1854-1863 yılları arasında İngiliz matematikçi Charles Baggage ve Avusturya Ordusunda görevli kriptograf Friedrich Kasishi tarafından kırılmıştır (Çimen vd., 2008).

1623: Sir Francis Bacon, 5-bit ikili kodlamayla karakter tipi değişikliğine dayanan stenografı buldu.

1790: ABD Başkanı Thomas Jefferson, matematikçi Dr. Robert Patterson yardımıyla günümüzde Jefferson Diski adıyla bilinen sistemi geliştirdi (Şekil 5). Bu sistemin benzeri 2. Dünya Savaşı'nda Amerikan ordusu tarafından kullanılmıştır. Mucit olan Thomas Jefferson Amerikan kriptolojisinin atası olarak adlandırılır.

Şekil 5. Jefferson diski (URL-5).

1817: Colonel Decius Wadsworth, üzerinde harflerin değişik numaralarla bulunduğu çarklardan oluşan bir şifreleme diski geliştirdi.

1854: Charles Wheatstone, Playfair olarak adlandırılan şifreleme yöntemini tasarladı.

1883: Hollandalı dilbilimci ve kriptograf Auguste Kerckhoffs'un yayınladığı *"La Cryptographie Militarie"* isimli makalesinde bir şifreleme sisteminde anahtar bilinmediği takdirde sistem ile ilgili her şey bilinse bile sistemin güvenliğinin tam olması gerektiğini söylemiştir. Kerckhoff Prensipleri şu şekildedir (Menezes vd., 1997).

- Sistem, pratik ve matematiksel bir gerçekliğe dayanmalıdır.
- Sistem gizliliğe dayanmalıdır. Yani sistem hakkındaki her şey herkes tarafından bilinmelidir.
- Sistemde kullanılan anahtarlar taraflar arasında kolayca, üçüncü kişinin değiştirmesine izin vermeden değiştirilebilmelidir.
- Sistem, telgraf uygulamasında kullanılabilmelidir.
- Sistemin kullanılabilmesi için fazla sayıda insana ihtiyaç duyulmamalıdır.
- Sistemin uygulaması ve anlaşılması kolay olmalı ve şifreleme sisteminin güvenliği, şifreleme algoritmasını gizli tutmaya dayanmalıdır; güvenlik, yalnızca anahtarı gizli tutmaya dayanmalıdır.

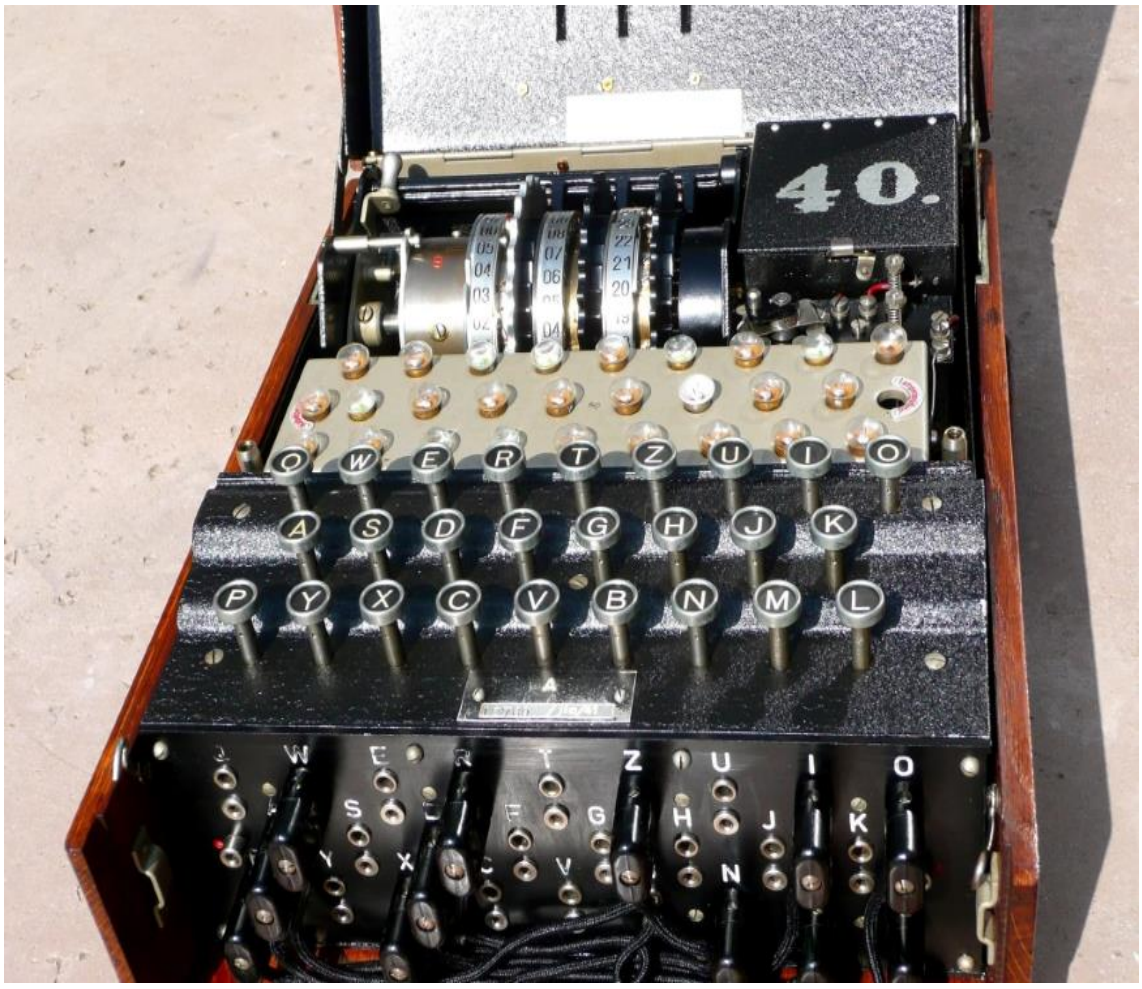
1917: İlk büyük etkili şifre kırma olayı Alman İmparatorluğu'nun Dışişleri Bakanı Arthur Zimmermann tarafından Meksika ve Washington'daki Alman Büyükelçilikleri üzerinden gönderilen şifrelerin çözülmesinde kendini gösterdi. Zimmermann Telgrafı (Zimmermann Note/Telegram) da olarak bilinen bu olayda, gönderilen telgraf Alman Dışişleri şifreleme standartlarına göre kodlanmıştı ve mesajda Meksika'yı Almanya'nın yanında, Amerika'nın karşısında bir savaşa davet ediyordu. Meksika'nın tavrına göre de Japonya'nın katılıp katılmayacağı bildiriliyordu. İki İngiliz şifre çözücünün mesaj içeriğini çözmeleri ve bunu ABD Başkanı Wilson'a okutmaları sonucunda 2 Nisan 1917'de ABD Birinci Dünya Savaşı'na katıldı (URL-6).

1917: Joseph Mauborgne ve Gilbert Vernam mükemmel şifreleme sistemi olan "one-time pad" i buldular (Vernam Şifreleme Yöntemi).

1918: Bir yer değiştirme ve ters çevirme karışımından oluşan ve telsiz haberleşmelerinde kullanılan ADFGVX şifresi Almanlar tarafından bulundu.

1929: Leste S. Hill 'in yayınladığı *"Cryptography In An Algebraic Alphabet"* adlı eserinde matematiğin şifrelemede ne kadar etkin kullanılabileceğini göstermiştir. Hill şifresi olarak adlandırılan bu yöntem lineer cebire dayanmaktadır.

1940-1944: İkinci Dünya Savaşı sırasında askeri alanda kullanılan şifreleme sistemleri ve bunların çözülmesinde kullanılan algoritmaların çeşitliliği de ve bu alana yapılan yatırımların artmasıyla Almanlar ENIGMA (Şekil 6-7), İngilizler TYPEX, Amerikalılar SIGABA, Japonlar RED&PURPLE gibi kriptoloji cihazları üretilmiş, ayrıca ENIAC (Şekil 8) ve COLOSSUS gibi ilk bilgisayar kabul edilen cihazlar bulunmuştur.

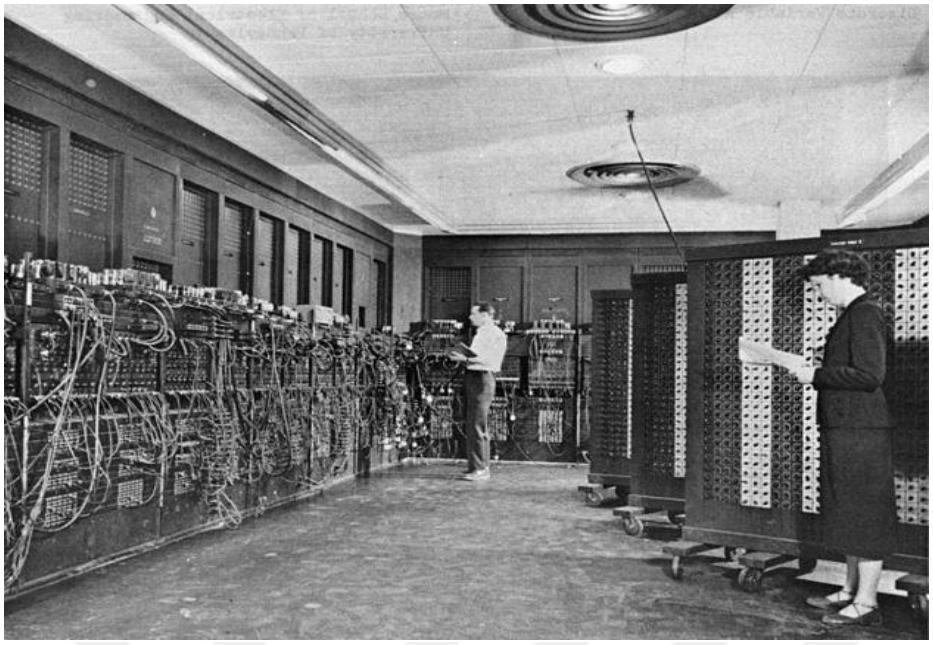


Şekil 6. Enigma (URL-7).

Enigmanın şifresini çözmek için zaman ile yarışılması gerekliydi çünkü şifre her gece yarısı değişmekteydi. İngiliz matematikçi ve kriptolog olan Alan Mathison Turing

tarafından tasarlanan Turing makineleri ve fikirleri ile geliştirilen Colossus bilgisayarı sayesinde enigmanın şifrelerinin kırılması sağlanmıştır.

Şekil 7. Enigma cihazı ile mesaj yollayan Alman askerleri (URL-8).



Şekil 8. ENIAC-ilk bilgisayar (URL-9)

1952: ABD'de resmi olarak Ulusal Güvenlik Teşkilatı olan NSA kuruldu.

1970: Dr. Horst Feistel öncülüğünde IBM laboratuvarlarında önce Demon daha sonra Lucifer denilen şifreleme sistemi geliştirildi. Lucifer, Veri Şifreleme Standardı olan DES'in temelini oluşturmaktadır. DES'in yapısı gereği şifreleme sisteminde kullanılan anahtarı hem alıcı hem de gönderici bilmek zorundaydı. Anahtarı ele geçiren herhangi birisi çok rahatlıkla düz metine ulaşabilirdi. Bu durum mesajlaşmadan önce anahtarın alıcı ve gönderici arasında güvenilir bir şekilde iletilmesi gerekliliğini ortaya çıkarmıştı (Çimen vd., 2008).

1976: Whitfield Diffie ve Martin Hellman bir algoritma tasarladılar. Bu algoritmaya göre alıcı ve göndericinin gizli bir anahtar üzerinde anlaşmaları için bir araya gelmeleri gerekmiyordu. Bu yeni durum anahtarlı kriptografi diye yeni bir tanımı ortaya çıkarıyordu. Bu tanıma göre artık herkesin birbirini tanımadan bile gizli bir şekilde haberleşebileceği demekti. Bu döneme kadar tasarlanan bütün kriptografilerde kullanılan anahtarın taraflarca bilinmesi gerekirken, artık kişilerin kendilerine ait özel anahtarları olabilecekti (Çimen vd., 2008).

1977: Kişilerin kendilerine ait özel anahtar olabileceği düşüncesinden etkilenen Ronald Rivest, Adi Shamir ve Leonard Adleman, RSA denilen şifreleme sistemini buldular. Bu sistem çarpanlara ayırma mantığıyla çalışmaktadır.

1980: Sezar şifresinin bir benzeri olan ROT13 şifreleme sistemi kullanılmaya başlandı.

1981: Kriptoloji üzerine ilk konferans, California Santa Barbara Üniversite'sinde CRYPTO 81 adı altında gerçekleştirildi.

1985: Neal Koblitz ve Victor S.Miller ayrı yaptıkları çalışmalarda ECC adı verilen eliptik eğri kriptografik sistemlerini tarif ettiler. Eliptik eğriler, şifreleme ve veri güvenliğinde tam değer vermeleri nedeniyle kullanışlıdırlar. Genelde gerçek sayı kümesinde çalışan fonksiyonlar yuvarlama veya belirsizlik durumlarından dolayı şifreleme sistemlerinde tercih edilmemektedirler.

1990: Xuejia Lai ve James Massey, IDEA algoritmasını buldular. 1991 yılında tasarlanmış bir blok şifreleme algoritmasıdır. Bu algoritmaya DES yerine üretilen PES'in geliştirilmiş hali denebilir. Bilinen en güçlü algoritmalardandır (URL-10).

1991: Phil Zimmerman, PGP sistemini geliştirdi ve yayınladı. Veri iletişimi için kimlik doğrulama ve mahremiyeti sağlayan bir veri şifreleme ve şifre çözme yöntemidir. PGP genellikle dosya imzalama, metin, e-posta, dosya, hard disk ve dizin şifreleme gibi iletişim güvenliğini artırma yöntemlerinde kullanılır.

1995: SHA-1 özel algoritması NIST tarafından standart olarak yayınlandı. Bu algoritma ile sadece şifreleme işlemi yapılır, şifre çözme işlemi yapılamaz.

2000: Belçikalı Joan Daemen ve Vincent Rijmen tarafından bulunan ve AES olarak adlandırılan yeni şifreleme sistemi bulunmuştur. Bu şifrelemenin bugüne kadar herhangi bir güvensizliği ispatlanamamıştır.

2009: Kriptografi konusunda dünyanın ilk olimpiyatları Belçika'nın Katholieke Üniversitesinde 25-28 Şubat tarihleri arasında yapılacak olan ön eleme ile başladı.

1.3. Tarihimizden Kriptoloji Örnekleri

Ülkemizde şifreleme ile ilgili pek fazla veri ve kaynak bulunmamaktadır. Ancak Kurtuluş Savaşı ve Kıbrıs Barış Harekâtı sırasında şifreleme teknikleri kullanılmıştır.

Selçuklular zamanında kullanılan Siyakat yazıları Türkler tarafından bulunan şifreli yazıya bir örnektir. Osmanlı Devleti bu yazıları genellikle tapu işlemlerinde kullanılırdı.

Kurtuluş Savaşı'nı sona erdiren Büyük Taarruz emrinin verildiği Afyonkarahisar'daki Türk istihbarat timleri çok basit bir steganografi örneğini kullanarak halk ile haberleşiyordu. Sinanpaşa ilçesi ve çevre köylerindeki düşman askerlerinden edinilen bilgileri Sandıklı'da bulunan Fahrettin Altay Paşa'ya istihbarat görevlileri ulaştırıyordu. Toplanan istihbarat bilgileri limon suyuyla kâğıt üzerine yazılıyor ve mektubun düşman askerlerinin eline geçmesi durumunda boş sanılarak dikkat çekmemesi sağlanıyordu. Beyaz kâğıt üzerine limon suyuyla yazılan bilgiler ateşe tutulduğunda görülür hale geliyor ve yetkili kişilerce okunabiliyordu. Limon suyuyla yazılan mektuplar, ekmekler içinde gerekli yerlere ulaştırılırken, okunduktan sonra ateşte yakılarak imha ediliyordu (Çimen vd., 2008).

Ülkemizde bilinen en önemli şifreli mesaj ise Kıbrıs Barış Harekâtı'nı başlatan mesajdır. CENEVRE Konferansı'na katılan Türk Dışişleri Bakanı Turan GÜNEŞ anlaşmanın mümkün olmadığını anlayınca, 13 Ağustos'ta "Ayşe tatile çıksın" parolasını Başbakan Bülent ECEVİT'e bildirdi. 'Ayşe' Turan Güneş'in kızının adıdır. Bunun üzerine hazırlıklarına başlayan Türk birlikleri iki gün sonra tekrar ilerlemeye başladı ve 16 Ağustos'ta Lefke ve Magosa'nın kurtarılmasıyla sona eren üç günlük İkinci Harekâtı'nı gerçekleştirdi (URL-11).

1.4. Türkiye'de Kriptoloji Tarihi

Türkiye'de şifreleme cihazları üzerine ilk çalışmalar 1970li yıllarda başlamıştır. TÜBİTAK'a bağlı çalışan Gebze'deki EAÜ'de TSK için yerli şifre cihazı üretme çalışmaları ile başlamıştır. 1978 yılında MİLON-I adı verilen prototip cihaz üretilmiştir. Daha sonraki süreçte MİLON-II adı verilen arazi şartlarına uyum sağlayabilen, taşınabilen ve sıralaşmalı haberleşme özelliğine sahip cihaz üretildi. MİLON serisi (Şekil 9) günümüzde 7. seriye kadar ulaşmıştır (Yılmaz, 2008).

Şekil 9. MİLON-4A, NATO envanterine giren ilk Türk kripto cihazı (URL-12).

Ülkemizde 2005 yılından itibaren Ortadoğu Teknik Üniversitesi'nde Ulusal Kriptoloji Sempozyumu düzenlenmeye başlanmasının yanı sıra çeşitli tez ve makalelerde yazılmıştır. Bunlardan bir kaçı şunlardır; Erhan (1993), tarafından yapılan çalışmada RSA algoritması kullanarak kişisel bilgisayarlarda dosya güvenliğini sağlamak amacıyla bir açık anahtar şifreleme yazılımı tasarladı. Gül (1997), tarafından yapılan çalışmada RSA tabanlı açık anahtarlı şifreleme sistemini kullanarak, ortak anahtarlı bir kripto sistem yazıldı. Soyalıç (2005), tarafından yapılan çalışmada verinin bütünlüğünü korumakta ve sayısal imza tasarılarında kullanılan Hash fonksiyonları ve uygulamalarını ayrıntılı olarak inceledi. Şiap (2008), tarafından yapılan çalışmada McEliece Şifreleme sistemi incelemiş ve matris kodlarını McEliece Şifreleme sistemine uyguladı. Karaahmetoğlu (2010), tarafından Gizli anahtarlı kripto sistemlerin tasarımında cebirsel yapıların önemi ve kriptanaliz konusu incelendi. Aslan (2013), tarafından yapılan çalışmada Blok şifreler için cebirsel ikili doğrusal dönüşüm tasarımı

ve modern bir blok şifreye uygulanması incelendi. Hassanpour (2015), tarafından asal sayıların şifreleme üzerindeki uygulamaları incelendi. Öztürkmenoğlu (2016), tarafından matrislerde şifreleme işlemleri incelendi.

1.5. Kriptoloji Terminolojisi

Bu bölümde kriptografik sistemlerde kullanılan tanımlar ve terminolojilerden bahsedilmiştir. Tanımlar ve terminoloji oluşturulurken (Külen, 2013; URL-13; Arslan, 2009; Soyalıç, 2005) çalışmalarından faydalanılmıştır.

Terminoloji: Bir sanat, bir bilim ya da bir teknik dalında özel olarak kullanılan terimlerin tümüne denir.

Kriptografi: Belgelerin şifrelenmesi ve şifresinin çözülmesi için kullanılan yöntemlere verilen isimdir.

Kriptanaliz: Kriptografik sistemlerin kurduğu mekanizmaları inceler ve çözmeye çalışan sistemdir.

Steganografi: Eski Yunanca 'da gizlenmiş yazı anlamına gelir ve bilgiyi gizleme bilimine verilen addır.

Şifreleme: Verinin veya bilginin kriptolaştırılması işlemidir.

Deşifreleme: Verinin veya bilginin kripto özelliğini yitirmesidir.

Şifreli Metin: Verinin standart ya da özel algoritmalar ile kriptolaşmasıdır.

Anahtar: Verinin çözümü için lazım olabilecek ipucudur.

Genel Anahtar: Herkesin görebileceği anahtardır.

Gizli anahtar: Verinin kriptolanmış halini görmek için iş yarayan anahtardır.

Gizlilik: Verinin, ona erişme hakkı olmayan üçüncü kişilerden uzak tutulmasıdır.

Özgünlük: Verinin üçüncü kişiler tarafından değiştirilmesinin engellenmesidir.

Anonimlik: Belirli işlemler için birimin kimliğinin saklanabilmesidir.

Gizlilik: Taşınan bilginin içeriğinin gizli kalmasıdır.

1.6. Matematiksel Kavramlar

Bu bölümde kriptografik sistemlerde kullanılan bazı matematiksel tanım ve teoremler verilmiştir. Tanım ve teoremler oluşturulurken (Altindiş, 1999; Erdoğan vd., 2008; Çallıalp, 2011; Balcı, 1999; Bilgiç, 2014) kaynaklarından yararlanılmıştır.

Teorem 1.1. $\mathrm{a}, \mathrm{b} \in \mathbb{Z}$ ve $b > 0$ olmak üzere $a = bq + r$ olacak şekilde, $0 \leq r < b$ şartını sağlayan bir tek q, r tam sayı ikilisi vardır.

Tanım 1.1. $\mathrm{a}, \mathrm{b} \in \mathbb{Z}$ olmak üzere $a.c = b$ olacak şekilde bir c tam sayısı varsa 'a, b yi böler ya da b, a ile bölünebilir' denir ve $a|b$ şeklinde gösterilir.

$\forall\, a, b, c$ sıfırdan farklı tam sayılar için aşağıdaki özellikler sağlanır.

- $a|a$ dır.
- $a|b$ ve $b|c$ ise $a|c$ olur.
- $a|b$ ve $\forall\, x \in \mathbb{Z}$ için $a|bx$ olur.
- Eğer $a|b$ ve $a|c$ ise $a|(b + c)$ ve $a|(b - c)$ olur.
- Eğer $a|b$ ve $b|a$ ise $a = b$ dir.

Tanım 1.2. $p > 1$ olmak üzere 1 den ve kendisinden başka böleni olmayan p sayısına asal sayıdır.

Tanım 1.3. $c|a$ ve $c|b$ ise c tam sayısına a ve b nin bir ortak böleni denir.

Tanım 1.4. Aşağıdaki özellikleri sağlayan negatif olmayan bir d tam sayısına a ve b nin en büyük ortak böleni denir ve $ebob(a,b)$ veya (a,b) ile gösterilir.

- d, a ve b nin en büyük ortak bölenidir.
- $c|a$ ve $c|b$ ise $c|d$ dir.

Teorem 1.2. d, a ve b tam sayılarının en büyük ortak böleni ise $d = (a,b) = ax + by$ olacak şekilde x, y tam sayıları vardır.

Tanım 1.5. $a, b \in \mathbb{Z}$ olmak üzere $(a,b) = 1$ şeklinde ise bu iki tam sayı birbirlerine göre asaldır denir .

Tanım 1.6. $m \in \mathbb{Z}^+$ olmak üzere $0 \leq x \leq m-1$ ve $(x,m) = 1$ şartını sağlayan x tam sayılarının sayısına m nin Euler sayısı denir ve $\varphi(m)$ ile gösterilir.

Tanım 1.7. A ve B iki küme olmak üzere, A dan B'ye olan bir f bağıntısı aşağıdaki özelliklere sahipse f ye A dan B'ye bir fonksiyon denir.

- $\forall x \in A$ için $(x,y) \in f$ olacak şekilde B'de en az bir y elemanı vardır.
- $(x,y) \in f$ ve $(x,z) \in f$ ise $y = z$ dir.

f, A dan B'ye bir fonksiyon ise $f: A \to B$ şeklinde gösterilir.

Tanım 1.8. $f: A \to B$ ye fonksiyonunda A kümesine tanım kümesi, B kümesine de değer kümesi denir.

Tanım 1.9. $f: A \to B$ ye fonksiyon ise A nın B altındaki görüntü kümesi $f(A) = \{ f(x): x \in A \}$ şeklinde tanımlanır.

Tanım 1.10. $f: A \to B$ ye fonksiyonu için, $f(A) = B$ ise f ye örten fonksiyon denir. f örten ise $\forall\, y \in B$ için $f(x) = y$ olacak şekilde en az bir $x \in A$ vardır.

Tanım 1.11. $f(x_1) \neq f(x_2)$ için $x_1 \neq x_2$ ise f ye birebir fonksiyon denir.

Tanım 1.12. $f: A \to B$ ye fonksiyon ve $Y \subset B$ ise A'nın $f^{-1}(Y) = \{a \in A: f(a) \in Y\}$ alt kümesine Y nin f altındaki ters görüntüsü denir.

Tanım 1.13. m bir pozitif tam sayı olmak üzere eğer $m|(a-b)$ ise a sayısı b tam sayısına m modülüne göre denktir denir ve $a \equiv b\ (mod\ m)$ şeklinde gösterilir.

Tanım 1.14. $\mathbb{Z}$ deki " $\equiv$ " denklik bağıntısının belirttiği denklik sınıflarına, m modülüne göre $(mod\ m)$ kalan sınıfları denir ve tüm kalan sınıfları kümesi $\mathbb{Z}_m$ ile gösterilir.

$a \in \mathbb{Z}$ nin denklik sınıfı, $\bar{a} = \{x \in \mathbb{Z}: m|(a-x)\}$ dir.

Teorem 1.3. $a, b, k \in \mathbb{Z}$ ve $n \in \mathbb{N}$ olmak üzere $a \equiv b\ (mod\ n)$ olsun. Bu durumda

- $a + k \equiv b + k\ (mod\ n)$
- $a - k \equiv b - k\ (mod\ n)$
- $a.k \equiv b.k\ (mod\ n)$

Tanım 1.15. Sonlu bir A kümesi verilsin. A dan A ya tanımlanan birebir ve örten dönüşüme bir permütasyon denir.

Tanım 1.16. G boş olmayan bir küme, " $*$ " G üzerinde tanımlı bir ikili işlem olsun. Eğer aşağıdaki şartlar sağlanıyorsa $(G,*)$ cebirsel yapısına bir grup denir.

- $\forall\, a, b \in G$ için $(a * b) \in G$ dir. (Kapalılık)
- $\forall\, a, b, c \in G$ için $(a * b) * c = a * (b * c) \in G$ dir.(Birleşme)
- $\forall a \in G$ için $(a * e) = (e * a) = a$ olacak şekilde bir $e \in G$ vardır. (Birim Eleman)

- $\forall a \in G$ için $(a * b) = (b * a) = e$ olacak şekilde bir $b \in G$ vardır. (Ters Eleman)

Tanım 1.17. $(G,*)$ bir grup ve $\forall a, b \in G$ için $(a * b) = (b * a)$ değişme özelliği sağlanıyorsa gruba değişmeli grup veya Abel grubu denir.

Önerme 1.1. $(\mathbb{Z}_m, +)$ cebirsel yapısı aşağıdaki özellikleri sağlarsa değişmeli gruptur.

- $\forall a, b \in \mathbb{Z}_m$ için $(a + b) \in \mathbb{Z}_m$ dir.($\mathbb{Z}_m$ toplama işlemine göre kapalıdır.)
- $\forall a, b \in \mathbb{Z}_m$ için $(a + b) = (b + a)$ dır. ($\mathbb{Z}_m$ toplama işlemine göre değişmelidir.)
- $\forall a, b, c \in \mathbb{Z}_m$ için $(a + b) + c = a + (b + c)$ dir. ($\mathbb{Z}_m$ toplama işlemine göre birleşimidir.)
- $\forall a \in \mathbb{Z}_m$ için $(a + 0) = (0 + a) = a$ dır. (Toplama işleminin birim elemanı 0 dır.)
- $a \in \mathbb{Z}_m$ için $a + (-a) = (-a) + a = 0$ olacak şekilde ters eleman mevcuttur.

Tanım 1.18. $ax \equiv b\ (mod\ n)$ şeklinde ki denkleme bir bilinmeyenli lineer denklem ve bu denklemi sağlayan x tam sayılar kümesine de denklemin çözümü denir.

Tanım 1.19. m tane satır ve n tane sütun oluşturacak biçimde dizilmiş mn tane sayının oluşturduğu tabloya bir $m \times n$ matris denir. $m \times n$ tipindeki bir A matrisi

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}_{m \times n} \quad \text{veya} \quad A = [a_{ij}],\ 1 \leq i \leq m\ ;\ 1 \leq j \leq n.$$

şeklinde gösterilir.

Tanım 1.20. $m \times n$ tipindeki bir A matrisi, c gibi bir skaler ile çarpılırsa bütün sayılar c skaleri ile çarpılır.

$A = [a_{ij}]_{m\times n}$ ve $c \in \mathbb{R}$ ise $c.A = [c.a_{ij}]_{m\times n}$

Tanım 1.21. A bir $n \times n$ matris ve I_n, $n \times n$ birim matris olmak üzere

$$A(A^{-1}) = (A^{-1})A = I_n$$

olacak biçimde bir A^{-1} $n \times n$ lik matrisi varsa bu matrise A matrisinin tersi denir.

Tanım 1.22. $a, b \in \mathbb{Z}_{26}$ olmak üzere $e(x) = ax + b\ (mod\ 26)$ ile tanımlanan fonksiyona Afin fonksiyonu denir.

Teorem 1.4. $p > 2$ bir asal sayı, e ise $(p-1)$ ile aralarında asal sayı olsun yani $(e, p-1) = 1$ koşulu sağlansın.

d sayısı, $e.d \equiv 1\ (mod\ p-1)$ koşulunu sağlayan bir sayı ise her $M \in \mathbb{Z}$ sayısı

$$M^{ed} \equiv M\ (mod\ p)$$

denkliği sağlanır.

Teorem 1.5. p ve q farklı asal sayılar, $e \in \mathbb{Z}, e \geq 1$ sayısı ise

$$\big(e, (p-1)(q-1)\big) = 1$$

eşitliğini sağlayan bir sayı olsun. d sayısı

$$e.d \equiv 1(mod\ (p-1)(q-1))$$

koşulunu sağlasın. Bu durumda M pozitif tam sayısı için

$M^{ed} \equiv M\ (mod\ pq)$ sağlanır.

2. YAPILAN ÇALIŞMALAR

Eski çağlardan beri haberleşmelerde gizlilik önemli bir sorun haline gelmiştir. Gizli tutulmak istenen her şey, bir sistem içerisinde değişik tarz ve yöntemler sayesinde şifrelenip alıcılara ulaştırılmıştır ve haberleşmenin en önemli araçlarından biri haline gelmiştir. Bir başka ifadeyle şifreler, özel bilgilerimizi korumanın en önemli yapı taşı haline gelmiştir. Bilgi güvenliği arttıkça kriptolojinin gücüne başvurulmuştur.

Şifre bilimi olarak da adlandırılan kriptolojinin; kriptografi ve kriptanaliz diye iki bölüme ayrılmaktadır.

2.1. Kriptografi

Tanım 2.1. Kriptografiyi Mao Wenbo şu şekilde tanımlamıştır (Wenbo, 2003) .

- Alfabetik karakterler dizisinden oluşan P açık metin uzayı,
- Şifreli metin mesajları kümesinden oluşan C şifreli metin uzayı,
- Olası şifreleme anahtarları kümesinden oluşan K şifreleme anahtar uzayı ve olası deşifreleme anahtarları kümesinden oluşan K' deşifreleme anahtar uzayı,
- Etkili bir anahtar planlama algoritması; $\gamma: N \rightarrow K \times K'$
- Etkili bir şifreleme algoritması; $\varepsilon: P \times K \rightarrow C$
- Etkili bir deşifreleme algoritması $\varepsilon' : C \times K' \rightarrow P$

Kriptografi için Stinson'a ait tanım ise şu şekildedir (Stinson, 2006)

Bir kriptografik sistem aşağıdaki koşulları sağlayan bir sıralı beşliden (P, C, K, E, D) oluşur.

- P; Düz metinlerin sonlu kümesidir.
- C; Şifreli metinlerin sonlu kümesidir
- K; Muhtemel anahtarların sonlu kümesidir

- $E = E_k : k \in K$ şifreleme ve $D = D_k : k \in K$ şifre çözme fonksiyonlarının kümesidir.
- Her $k \in K$ için bir şifreleme fonksiyonu $E_k \in E$ ve buna bağlı olarak bir şifre çözme fonksiyonu $D_k \in D$ vardır. Burada $E_k : P \to C$ ve $D_k : P \to C$ fonksiyonları her $x \in P$ için,

$D_k\, E_k\, x = x$ eşitliğini sağlarlar.

Kriptografi şu şekilde çalışır (Külen, 2013).

Adım 1. Gönderilecek mesaj belirlendikten sonra sistemde kullanılmak üzere alıcı ve göndericinin bildiği $k \in K$ olacak şekilde sistemin anahtarı belirlenir.

Adım 2. Gönderilecek mesajın sayısal karşılığı bulunarak sayı dizisi elde edilir. Yani $x_i \in P$ için $x_i = x_1 x_2 \ldots x_n$ sayı dizisi şeklindedir. (n≥ 1 ve $1 \leq i \leq n$)

Adım 3. $y_i = E_k x_i$ formülü ile her bir x_i düz metnine karşılık bir y_i değeri bulunur ve $y_i = y_1 y_2 .. y_n$ sayı dizisi elde edilir. Bu dizi şifreli metinin sayısal karşılığıdır.

Adım 4. $y_i = y_1 y_2 .. y_n$ şifreli metnine karşılık $x_i = D_k\, y_i$ fonksiyonu ile düz metne karşılık gelen $x_i = x_1 x_2 \ldots x_n$ sayı dizisi elde edilir.

Adım 5. $x_i = x_1 x_2 \ldots x_n$ sayı dizisi ile düz metin elde edilir.

Şifreleme sistemlerinde genel olarak İngiliz alfabe sistemi temel alınarak yapılmıştır ve $(mod\ 26)$ kullanılmıştır. Ancak; şifreleme yapılırken kullanılacak dilin alfabedeki harf sayısı dikkate alınmalıdır. Bu çalışmada Türk alfabetik sistemini (Tablo 2) kullanacağız. Sistemler Türk alfabesi için $(mod\ 29)$ kullanarak oluşturulacaktır.

Tablo 2. Türk alfabesinin sayısal karşılığı.

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	
15	16	17	18	19	20	21	22	23	24	25	26	27	28	

Şifreleme ve şifre çözme işleminde kullanılan birçok algoritma, teknik ve yaklaşım bulunmaktadır. Ancak sağlıklı ve güvenilir bir şifreleme için sağlanması gereken bazı kriterler vardır. Bunların bazıları şu şekildedir (URL-14).

- Şifrelenmiş mesaj, deşifre edildiğinde bilgi kaybı olmamalıdır.
- Şifreleme işlemlerinde güvenlik seviyesi mümkün olduğunca yüksek olmalıdır.
- İhtiyaç duyulan güvenlik seviyesine göre güvenlik seviyesi seçilebilmelidir.
- Şifrelenmiş mesaj ile düz metin arasındaki ilişki zor kurulmalıdır.
- Şifreleme işlemleri basitçe ve kolaylıkla gerçekleştirilebilmelidir.
- Verimi düşürecek, maliyeti ve işgücünü arttıracak yaklaşımlar içermemelidir.
- Kullanılan algoritmaların karıştırıcı özelliği olmalıdır.
- Şifreleme yaklaşımları herkese açık olmalıdır.
- Şifreleme yaklaşımları, açıklarının ortaya çıkarılabilmesi için mümkün olduğunca geniş bir platformda test edilebilmelidir.

Genel olarak şifreleme algoritmalarını; anahtar sayısına, mesaj tipine veya algoritmasına göre sınıflandırmak mümkündür. Bu çalışmada, kriptografik şifreleme sistemlerini simetrik (gizli anahtar), asimetrik (açık anahtar) ve karışık şifreleme olarak üçe ayrılacaktır. Simetrik ve asimetrik şifrelemelerin yanı sıra, aslında bir simetrik şifreleme çeşidi olan geleneksel (klasik) kriptografik sistemleri de ayrı bir başlık olarak incelenecektir.

2.1.1. Simetrik (Gizli Anahtar) Şifreleme Yöntemleri

Simetrik şifre algoritmalarında şifreleme ve deşifreleme işlemleri için tek bir anahtar kullanılmaktadır. Sistemin güvenliği tamamen şifreye bağlı bir durumdur. Şifreleme işlemi gerçekleştirildikten sonra şifreli metin alıcıya gönderilirken anahtar da alıcıya güvenli bir şekilde gönderilmelidir. Şifreleme ve deşifreleme işlemleri hızlı bir şekilde gerçekleştirme imkânı vardır.

Tablo 3. Çeşitli simetrik şifreleme çeşitleri (Kodaz, 2010).

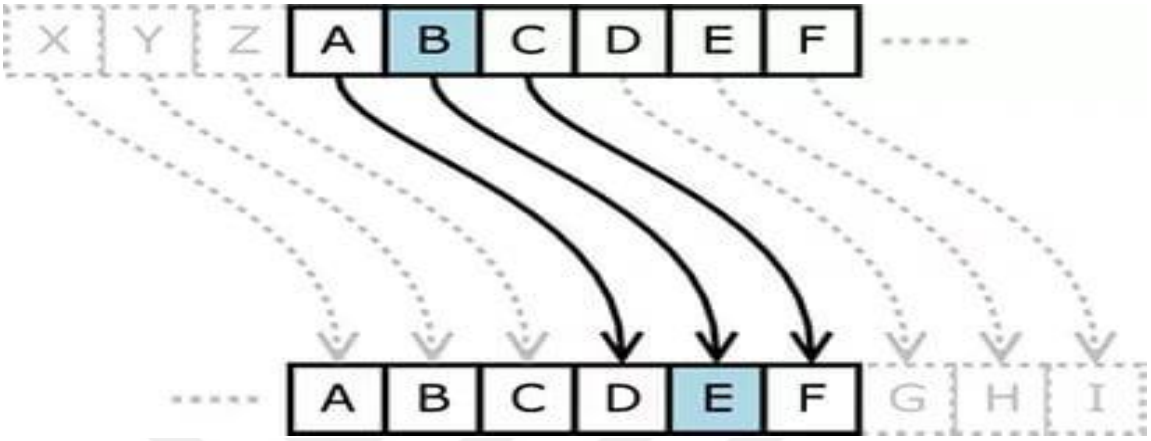
Algoritmanın Adı	Geliştiren	Tarihi
LUCİFER	IBM (ABD)	1970
DES	IBM (ABD)	1977
FEAL	SHİMİZU VE MİYAGUCHİ (JAPONYA)	1988
GOST 28147-89	I.A.ZABOTİN, G. P. GLAZKOV, V.B.ISAEVA (SOVYETLER BİRLİĞİ)	1989
IDEA	LAİ-MASSEY, ETH ZURİCH (İSVİÇRE)	1992
BLOWFISH	BRUCE SCHNEİER, COUNTERPANE SYSTEMS (ABD)	1993
SAFER	MASSEY, CYLİNK CORPORATİON (ABD)	1993
SKİPJACK (CLİPPER ŞİFRESİ)	NSA (ABD)	1993
ASEKAL-21	ASELSAN (TÜRKİYE)	--

2.1.2. Klasik Kriptografik Sistemler

Bir çok kripto sisteminde bir anahtar seçildikten sonra, açık metindeki her bir harf şifreli metindeki tek bir harfe dönüşür. Bu tip kripto sistemlerine mono alfabetik kripto sistemler denir. Aksine her bir harfin farklı harflere dönüştüğü sistemlere ise mono alfabetik sistemler denir.

Geçmişten günümüze kadar kullanılan geleneksel (klasik) kriptografik sistemlerin en yaygın olanları bu kısımda incelecektir.

2.1.2.1. Sezar Şifresi (Kaydırma Şifreleyicisi)



Şekil 10. 3 harf ileri kaydırılmış Sezar şifreleme (URL-15).

Tarihin ilk kriptolojik fikirleri İngilizcede transposition and substitution cipher adını taşıyan yer değiştirme ve harf değiştirme şifrelemeleridir. Bu yöntemlerden ilki bir yazıdaki harflerin yerlerini değiştirerek, ikincisi ise harfleri başka harflerle değiştirerek elde edilir. Bu şifreleme yöntemiyle kullanan en ünlü teknik Sezar Şifresi'dir.

Sezar şifrelemede, açık metini oluşturan her harf kendinden sonraki 3. harfe kaydırılması metoduna dayanan bir şifreleme yöntemidir (Şekil 10). Genel olarak sayısal değeri gösterimi yapılan açık metni oluşturan harflere karşılık gelen değere, belli bir değer eklenerek şifreli metin bulunur. Eklenen değer anahtar değeridir. Açık metin, şifreli metindeki harflere karşılık gelen sayısal değerden anahtarın çıkarılması ile elde edilir.

Sezar Şifreleme işlemi yapılırken Tablo 4 deki algoritma kullanılır. Her harfin Tablo 2 yardımıyla sayısal değeri bulunduktan sonra k anahtar değeri eklenir, $(mod\ 29)$ a göre işleme sokulduktan sonra şifreli mesajın sayısal değeri bulunur. Yine Tablo 2 yardımıyla sayısal değerin harf karşılığı bulunur. Mesajı deşifrelemek için

eklenen k anahtar değeri sayısal karşılıktan çıkarılıp, aynı işlemlere tabi tutulur (Stinson, 2006).

Tablo 4. Sezar şifreleme algoritması

$0 \leq k \leq 28$ için
$E_k\ (x) = x + k\ (mod\ 29)$
$D_k\ (x) = x - k\ (mod\ 29)$

Örnek 2.1. "ÇUKİTA" kelimesini k=10 olacak şekilde şifreli halini bulmak için; öncelikle Tablo 2 yardımıyla kelimenin sayısal değeri bulunur. Daha sonra anahtar değeri olan k=10 kullanarak, her sayısal değere 10 eklenerek $x + 10\ (mod\ 29)$ şifreleme fonksiyonu bulunur. $(mod\ 29)$ a göre işlem yapıldıktan sonra, yeni sayısal değerlerin Tablo 2 yardımıyla karşılığı bulunur.

Açık Metin	Ç	U	K	İ	T	A
Sayısal Değer	03	24	13	11	23	00
$E_{10}(x) = x + 10\ (mod\ 29)$	13	05	23	21	04	10
Şifreli Metin	K	E	T	S	D	I

ÇUKİTA kelimesinin k=10 anahtarı ile şifrelenmiş hali KETSDI kelimesidir.

Şifreli metinin sayısal karşılığından k=10 anahtarı çıkarılınca $x - 10\ \ (mod\ 29)$ deşifreleme fonksiyonu yardımıyla anahtar metine ulaşılır.

Şifreli Metin	K	E	T	S	D	I
$Sayısal\ Değer$	13	05	23	21	04	10
$D_{10}(x) = x - 10\ (mod\ 29)$	03	24	13	11	23	00
Açık Metin	Ç	U	K	İ	T	A

Sezar şifreleme yöntemi güvenli olmayan yöntemler arasındadır. Çünkü kriptanalizi kolayca yapılabilir. Alfabedeki harf sayısı kadar kriptanaliz anahtarı vardır.

Türkçeye harf sistemine göre Sezar şifreleme yöntemi ile şifrelenmiş bir metin 29 farklı deneme yapılarak çözülebilir.

2.1.2.2. Yer Değiştirme Şifreleyicisi

Sonlu bir X kümesi üzerinde tanımlanan bir birebir ve örten $\varphi: X \rightarrow X$ permütasyonu aracılığı ile şifreleme gerçekleşir. k anahtarı o dildeki bütün sembollerin karşılığı olacak kadar permütasyon içerir. Her φ permütasyonunun φ^{-1} ters permütasyonu vardır (Stinson, 2006).

Yer değiştirme şifreleyicisinde Tablo 2 ye göre sayısal karşılığı bulunan her harfin karşılığı verilen permütasyon yardımıyla bulunur ve yer değiştirme işlemi yapılır. Aynı şekilde deşifreleme işlemide gerçekleştirilir. Tablo 5 de yer değiştirme şifresinin algoritması verilmiştir.

Tablo 5. Yer değiştirme şifre algoritması.

$P, C \in \mathbb{Z}_n$ ve $\varphi = k$ için
$E_\varphi(x) = \varphi(x)$
$D_\varphi(x) = \varphi^{-1}(y)$

Örnek 2.2.

$$\varphi = \begin{pmatrix} 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17\ 18\ 19\ 20\ 21\ 22\ 23\ 24\ 25\ 26\ 27\ 28 \\ 4\ 9\ 0\ 8\ 3\ 2\ 1\ 6\ 5\ 7\ 28\ 19\ 11\ 10\ 20\ 27\ 12\ 26\ 15\ 22\ 25\ 18\ 16\ 13\ 21\ 24\ 17\ 14\ 23 \end{pmatrix}$$

permütasyonu ile açık metni "LAZBÖREĞİ" olan kelime şu şekilde şifrelenir. Burada φ permütasyonunda $0 \rightarrow 4$ olduğundan Tablo 2 yardımıyla A→D ye dönüşür. Benzer şekilde;

L→R A→D Z→T B→H Ö→M R→Ü E→B Ğ→E İ→P

şeklinde bulunur. Bütün dönüşümler yapıldıktan sonra "LAZBÖREĞİ" açık metni "RDTHMÜBEP" şifreli metnine dönüşür.

Deşifreleme için kullanılacak olan ters permütasyon, φ permütasyonunda ki satırların yer değiştirmesiyle elde edilir. Ters permütasyon şu şekildedir.

$$\varphi^{-1} = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15\,16\,17\,18\,19\,20\,21\,22\,23\,24\,25\,26\,27\,28 \\ 2\,6\,5\,4\,0\,8\,7\,9\,3\,1\,13\,12\,16\,23\,27\,18\,22\,26\,21\,11\,14\,24\,19\,28\,25\,20\,17\,15\,10 \end{pmatrix}$$

φ^{-1} permütasyonunda $0 \rightarrow 2$ olduğundan Tablo 2 yardımıyla A→C ye dönüşür. Şifreli metinin bütününe uygulanınca

R→L D→A T→Z H→B M→Ö Ü→R B→E E→Ğ P→İ

şeklinde olur. Açık metin olan LAZBÖREĞİ metnine ulaşılır.

Yer değiştirme şifreleyicisinde kriptanaliz yapmak için n harfe sahip olan bir dil için k anahtarını $n!$ tane olabilir. Örneğin Türkçe için anahtar sayısı 29! dir. Bu kadar büyük anahtar araması yapmak oldukça güçtür.

2.1.2.3. Polybius'un Dama Tahtası

Tarihte Skytaleden sonra karşımıza çıkan kriptografik örneklerden biri de Polybius'un dama tahtası şifrelemesidir. Yunanlılar tarafından M.Ö. 205-123 yılları arasında Yunan tarihçisi Polybius tarafından tasarlanan bu sistemde kullanılan şifreleme alfabesi Yunan ve Roma alfabesiydi. Polybius'un dama tahtası, elemanları harfler olan 5×5'lik bir matristen oluşmaktaydı.

Kural şu şekildedir; Alfabe sırayla matrisin satırlarına yazılır ve her harfi belirleyen iki rakam vardır; ilk rakam bulunduğu satırı, ikinci rakam bulunduğu sütunu temsil eder. Her harf için bir sayı elde edilir. Türk alfabe sisteminden ötürü 5×6 tipinde matris (Tablo 6) kullanılmıştır (Çimen vd., 2008).

Tablo 6. Polybius dama tahtası

	1	**2**	**3**	**4**	**5**	**6**
1	A	B	C	Ç	D	E
2	F	G	Ğ	H	I	İ
3	J	K	L	M	N	O
4	Ö	P	R	S	Ş	T
5	U	Ü	V	Y	Z	

Örnek 2.3. Türkçe alfabe sistemini kullanarak "43-46-16-52-34-11-46-16-34-11-46-26-32-12-41-33-52-34-52" şifresi Polybius Dama Tahtası yardımıyla şu şekilde çözülür.

Polybius Dama Tahtası kuralı gereği birinci rakam satırı, ikinci rakam sütünü temsil etmektedir yani;

11→A 12→B ……..……..54→Y 55→Z

olarak eşleşir.

Şifrelenmiş sayılar Tablo 6 yardımıyla tek tek açılırsa;

43→R	46→T	16→E	52→Ü	34→M
11→A	46→T	16→E	34→M	11→A
46→T	26→İ	32→K	12→B	41→Ö
33→L	52→Ü	34→M	52→Ü	

Tablodan her sayının karşılık geldiği harf bulunduktan sonra aşağıdaki düz metin elde edilir.

"RTEÜ MATEMATİK BÖLÜMÜ"

Tam tersi olarak düz metinden şifreli sayıları oluşturmak için her harfin karşılık geldiği değer, Tablo 6 yardımıyla bulunur. Satır ve sütun kesiştirmesi yapıldıktan sonra, önce satırdaki sonra sütundaki rakam yazılır.

R→43 T→46 E→16 Ü→52

gibi diğer harfler içinde uygulanırsa "43-46-16-52-34-11-46-16-34-11-46-26-32-12-41-33-52-34-52" şifresi elde edilir.

2.1.2.4. Bifid ve Trifid Şifreleme Sistemi

Ünlü Kripto tarihçisi David Khan'ın da " Kriptolojide hatırı sayılır derecede önemli bir sistem icat etti (Khan, 1996). " diye belirttiği Fransız Felix Delastelle'in 1901 yılında bulduğu Bifid ve Trifid Şifreleme sistemi, çalışma mantığı açısından Polybius Dama Tahtası sistemine benzemektedir.

Bifid şifreleme sisteminde; Seçilen 5×5 tipindeki matriste satır ve sütunlar numaralandırılır. Rastgele seçilen bu matriste harfler sırayla veya karışık olarak matrise yerleştirilir. 5×5 olabileceği gibi daha büyük kare matrislerde olabilir. Metin yazılır ve genelde matrisin boyutu kadar parçaya ayrılır. Her harfin altına önce satır sonra da sütün numaraları yazılır. Elde edilen rakamlar grup içinde ilk satırdan başlayarak soldan sağa doğru bütün oluşturacak şekilde ikişerli olarak yazılır ve matristen her ikilinin karşılığı olan harf bulunur ve ortaya şifreli metin çıkar. Deşifreleme işlemi yapılırken harflerin karşılığı olan rakamlar yan yana yazılır (URL-16).

Örnek 2.4.1.

	1	2	3	4	5	6
1	G	.	B	K	P	İ
2	O	A	V	.	E	Ş
3	Ü	M	T	Y	L	H
4	F	Z	U	D	R	Ğ
5	N	J	C	S	I	.
6	Ç	Ö	.	.	.	.

Yukarıdaki 6×6 matrisi yardımıyla BİFİD ŞİFRELEME SİSTEMİ yazısı şu şekilde şifrelenir.

Açık metni 6 li gruplara bölüp, altına önce satır sonrada sütun numaraları yazılır.

B	İ	F	İ	D	Ş		İ	F	R	E	L	E		M	E	S	İ	S	T		E	M	İ
1	1	4	1	4	2		1	4	4	2	3	2		3	2	5	1	5	3		2	3	1
3	6	1	6	4	6		6	1	5	5	5	5		2	5	4	6	4	3		5	2	6

Bu işlemden sonra grup içinde kalınarak soldan sağa doğru rakamlar yeniden yazılır ve birleştirilir.

114142361646 144232615555 325153254643 231526

Bulunan bu rakamlar ikili gruplar halinde, ilk rakam satır ikinci rakam sütün olacak şekilde matris kullanarak harf karşılıkları bulunur.

11	41	42	36	16	46		14	42	32	61	55	55
G	F	Z	H	İ	Ğ		K	Z	M	Ç	I	I

32	51	53	25	46	43		23	15	26
M	N	C	E	Ğ	U		V	P	Ş

Yapılan işlem sonunda GFZHİĞ KZMÇII MNCEĞU VPŞ şifreli metni elde edilir.

Deşifreleme işleminde mantık tam tersi olarak işler. Yapılan her işlemin tersi yapılarak açık metin elde edilir.

Trifid Şifreleme Sistemi; Bifid Şifrelemeyi 3 boyuta taşımak için tasarlanmış bir yöntemdir. Her sembolün ikiye bölünmesi yerine üçe bölünmesini sağlar. Bifid Şifreleme veya Polybius Dama Tahtası sisteminde matrislerimiz 5×5 veya 6×6

tipinde matrisler iken Trifid Şifreleme Sisteminde $3 \times 3 \times 3$ lük bir küp kullanılır (URL-17).

Küpün x, y, z koordinatları göz önüne alınırsa her harfin $x_1\, y_1\, z_1$ gibi bir koordinatı olacaktır. Önce bulunduğu tabaka sayısı, ardından sütun sayısı ve son olarak da satır sayısı yazılır. Ardından şifrelemek istenilen mesajdaki bütün harflerin sayı değerleri yukarıdan aşağıya doğru yazılarak 3 satırlı bir matris elde edilir. Son olarak yukarıdan aşağıya yazılı olan bu sayı değerleri soldan sağa doğru okunarak şifreli mesajın sayı değerleri elde edilir ve her 3 sayı bir harfe karşılık gelecek şekilde şifrelenir.

Örnek 2.4.2.

1.TABAKA

	1	2	3
1	G	V	M
2	A	X	R
3	Q	L	E

2.TABAKA

	1	2	3
1	N	W	D
2	S	P	U
3	H	B	K

3.TABAKA

	1	2	3
1	Y	C	I
2	J	O	.
3	F	T	Z

Yukarıdaki matrisleri kullanarak TÜRKİYE kelimesini Trifid şifrelemeye göre şu şekilde şifrelenir. Önce şifrelenecek kelimenin altına koordinatlar dik bir şekilde yazılır ve rakamlar satır içinde sırasıyla yazılır ve elde edilen sayıların matristen karşılığı bulunu değerleri yazılır.

T	Ü	R	K	İ	Y	E
3	2	1	2	3	3	1
2	3	3	3	3	1	3
3	2	2	3	1	1	3
321	233	123	333	133	223	113
C	K	L	Z	E	B	Q

TÜRKİYE açık metninin şifrelenmiş hali CKLZEBQ kelimesi olarak elde edilir.

2.1.2.5. Playfair Şifresi

1854 yılında Charles Wheatstone ve Baron Lyon Playfair'in bulduğu şifreleme yöntemlerinden biridir. İngiliz alfabesine göre oluşturulan bu sistemde, 5×5 tipinde bir matris kullanılmaktaydı. İngilizce de I ve J az bulunduğundan dolayı, bu iki harf yan yana düşünülerek matris oluşturulmuştur. 20. yüzyılın başlarına kadar güvenliği korusa da, harf analizi yapılarak deşifre edilmiştir (Çimen vd., 2008).

Sistem şu şekilde çalışır;

- Seçilen anahtar kelimede ki birden fazla kullanılan harfler atılır ve matriste soldan itibaren yazmaya başlanır. Diğer kısımlara alfabenin kalan harfleri yazılır.
- Düz metin ikili gruplara ayrılır. Şifrelenecek mesaj tek sayıda harften oluşuyorsa, mesajın sonuna istenilen bir harf eklenir.
- İkili gruplardaki harfler aynı satırda ise sağlarındaki harflerle şifrelenir.
- İkili gruplardaki harfler aynı sütunda ise bir alt satırdaki harflerle şifrelenir.
- İkili harfler aynı satırda veya sütunda değil ise, ilk harfi şifrelemek için bu harfin bulunduğu satır ve ikinci harfin bulunduğu sütunun kesimindeki harf alınır. İkinci harfi şifrelemek için bulunduğu sütun ile ikinci harfin bulunduğu satırın kesişimindeki harf alınır.

Örnek 2.5. Türk alfabe sistemi kullanılarak ENGİN anahtarı yardımıyla TÜRK ALFABESİ açık metni şu şekilde şifrelenir.

Kural gereği anahtar kelimesinden aynı harfler atılır ve matris oluşturulur. Açık metin ikili gruplara dönüştürülüp şifreleme yapılır.

E	N	G	İ	A
B	C/Ç	D	F	Ğ
H	I	J	K	L
M	O/Ö	P	R	S/Ş
T	U/Ü	V	Y	Z

Düz Metin	TÜ	RK	AL	FA	BE	Sİ
Şifreli Metin	UV	YR	ĞS	Ğİ	HB	RA

TÜRK ALFABESİ açık metni ENGİN anahtarı yardımıyla UVYRĞSĞİHBRA olarak şifrelenir.

Mesajı çözmek için harfler aynı satırda ise soldaki harf, aynı sütunda ise üstteki harf alınır. Diğer yöntem aynen uygulanır.

2.1.2.6. Affine Şifreleme Sistemi

Bir yerine koyma şifreleyicisi olduğu da söylenebilen Affine Şifreleme Sisteminde Tanım 1.22 gereği hangi harfin hangi harfe karşılık geleceği bir formülle belirlenmiştir. İngiliz alfabe sistemine göre kurulan sistemin mantığı Tablo 7 de verilmiştir.

Tablo 7. Affine şifreleme algoritması

$P = C = \mathbb{Z}_{26}$
$K = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : (a,26) = 1\}$
$k = (a,b) \in K$ ve $\forall\, x,y \in \mathbb{Z}_{26}$ için
$e_k(x) = ax + b \ (mod\ 26)$
$d_k(y) = a^{-1}(y-b) \ (mod\ 26)$

Birebir bir Afin fonksiyonu için, n kullanılan dilin harf sayısı olmak üzere

$P = C = \mathbb{Z}_n$ ve $k = a, b \in \mathbb{Z}_n$ olsun.

$a, b \in \mathbb{Z}_n$ ve $(a, n) = 1$ olmak üzere şifreleme fonksiyonu

$e_{(a,b)}x = ax + b \ (mod\ n)$

olarak tanımlanır.

Seçilen Afin fonksiyonu birebir olduğundan

$y \in \mathbb{Z}_n$ için $ax + b = y \ (mod\ n)$

denklemi x için tek bir çözüme sahip olması gerekir. Bu denklem

$ax = y - b \ (mod\ n)$

denklemine denk bir denklemdir.

Bu denklemin çözümünün olması için gerek ve yeter şart $(a, n) = 1$ olmasıdır. $(a, n) = 1$ olduğunu kabul edersek, a nın mod n de tersi vardır ve bu

$x = a^{-1}\ (y - b)\ \ (mod\ n)$ olur.

Böylece $k = (a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n : (a, n) = 1$ ve $k = a, b \in \mathbb{Z}_n$ olmak üzere;
$\forall\, x, y \in \mathbb{Z}_n$ için;

$e_k\ (x) = ax + b \ (mod\ n)$ ve $d_k\ (y) = a^{-1}(y - b)\ (mod\ n)$
elde edilir.

Afin şifreleme sisteminde hangi dilde mesaj gönderilecekse o dilin standart alfabe sayısı kullanılır. İhtiyaç duyulduğu zamanlarda noktalama işaretleri, sayılar ve semboller de kullanılabilir.

Örnek 2.6. $k = (5,3)$ anahtarı ile 'MATEMATİK' açık metnini Afin Şifreleme yöntemi ile şu şekilde şifrelenir.

k anahtarı 5,3 olduğundan $a = 5$ ve $b = 3$ dir. $5,3 \in \mathbb{Z}_{29}$ ve $(5,29) = 1$ dir. $\forall\, x \in \mathbb{Z}_n$ için şifreleme fonksiyonu

$e_k\,(x) = 5x + 3\ (mod\ 29)$ olur.

Deşifreleme fonksiyonu için a^{-1} değerinin bilinmesi gerekir. Burada

$k = 5,3 \in \mathbb{Z}_n$ için $(5.a^{-1}) = 1\ (mod\ 29)$ olması gerekir. $a^{-1} = 6$ olduğu kolayca görülebilir. Deşifreleme fonksiyonu

$\forall\, y \in \mathbb{Z}_n$ için $d_k\,(y) = 6y - 18\ (mod\ 29)$ olur.

Şimdi "MATEMATİK" açık metnini Tablo 2 yardımıyla $k = 5,3$ anahtarını kullanarak şu şekilde şifrelenir.

Düz Metin	M	A	T	E	M	A	T	İ	K
x	15	0	23	5	15	0	23	11	13
$e_k\,(x) = (5x + 3)\ (mod\ 29)$	20	3	2	28	20	3	2	0	10
Şifreli Metin	R	Ç	C	Z	R	Ç	C	A	I

'MATEMATİK' açık metninden 'RÇCZRÇCAI' şifreli metnini elde edilir.

Benzer şekilde şifreli metinden düz metni elde etmek için $d_k\,(y)$ fonksiyonunu kullanılır.

Şifreli Metin	R	Ç	C	Z	R	Ç	C	A	I
y	20	3	2	28	20	3	2	0	10
$d_k\,(y) = \,(6y - 18)\,(\text{mod } 29)$	15	0	23	5	15	0	23	11	13
Düz Metin	M	A	T	E	M	A	T	İ	K

Affine fonksiyonu ile şifrelenmiş bir metnin şifresini kırmak için $k = (a, b)$ anahtarını bulmak gerekir. Kullanılan dildeki harf sayısı n olmak üzere tüm alternatifleri anlamlı bir metin elde edene kadar denemek gerekir. Ancak bilgisayar aracılığıyla bu kriptanaliz yapılabilir. Bir diğer yöntem ise frekans analiz yöntemidir.

2.1.2.7. Mors Alfabesi

Mors Alfabesi 1832'de telgraf ile ilgilenmeye başlayan Samuel Morse tarafından 1835 yılında oluşturulmuş ve 1837'de kullanılmaya başlanmıştır. Modern Uluslararası Mors Kodu ise, 1848 yılında Alman Friedrich Clemens Gerke tarafından geliştirilmiştir.

Mors kodu; sesli olarak, radyo sinyallerinin açılıp kapatılmasıyla, telgraf tellerinden geçen elektrik akımıyla, mekanik yolla ya da görsel (ışıkların yanıp sönmesi) yollarla iletilebilen bir şifreleme sistemidir. Kısa, uzun işaretler (nokta ve çizgiler) ve duraklamalardan oluşan bir alfabedir. Kısa ve uzun sinyallerin dışında aralardaki sessizlikler de anlam taşımaktadır. Örneğin; kısa aralık harfler arasında, orta uzunlukta aralık kelimeler arasında ve uzun aralıklar ise cümleleri birbirinden ayırmakta kullanılır.

Gönderici (verici) cihazın başındaki memur, "maniple" diye tanımlanan bir kola, kısa veyahut uzun basışlar yapar. Kısa basışlar nokta (.),uzun basışlar çizgi karşılığıdır. Böylelikle, yan yana gelen nokta ve çizgilere göre harfler, bunlardan da kelimeler, tümceler oluşur. Telgraf iletisinin alındığı yerde (alıcı cihazda), rulo halindeki bir kâğıt şerit dönmektedir. Bunun karşısında da, verilen işaretlere göre hareket eden bir kalem vardır. Bu kalem, nokta ve çizgileri kâğıt üzerinde çizer. Böylelikle kelimeler, tümceler alana gelir (URL-18).

Mors alfabesi bir sembolleştirme sistemidir. Bu sistemde hece harfleri yerine başka semboller kullanılır. Sembolleştirme sistemi Tablo 8 de gösterilmektedir.

Tablo 8. Mors alfabesi (URL-19).

A	._	J	._ _ _	S	...
B	_...	K	_._	T	_
C	_._.	L	._..	U	.._.
D	.._	M	_ _	V	..._
E	.	N	_..	W	._ _
F	_ _ _.	O	_ _ _	X	_.._
G	_.	P	._ _.	Y	_._ _
H	....	Q	_ _._	Z	_ _..
I	..	R	._.		
0	_ _ _ _ _	1	._ _ _ _	2	.._ _ _
3	…_ _	4	…._	5	…..
6	_....	7	_ _ …	8	_ _ _..
9	_ _ _ _.				
Nokta (.)	._._._	Virgül (,)	_ _.. _ _	Tire (-)	_...._
Soru İşareti(?)	.._ _..	Taksim (/)	_.._	İki nokta (:)	_ _ _...

Örnek 2.7. "HEMŞİN YAYLALARI" açık metni Mors Alfabesi ile şu şekilde şifrelenir.

Mors Alfabe Sistemi gereği her harfin yerine Mors sembolleri yerleştirilerek açık metin dönüştürülür. Tablo 8 yardımıyla açık metin şu şekilde şifrelenir;

Açık Metin: HEMŞİN YAYLALARI

Şifreli Metin: .... . _ _ … .. _.. _._ _ ._ _._ _ ._.. ._ ._.. ._ ._. ..

2.1.2.8. ADFGVX Şifrelemesi

Alman ajanı Fritz Nebel tarafından 1. Dünya savaşı sırasında geliştirilen ADFGX ve ADFGVX şifre algoritmalarının amacı telsiz iletişimini güvence altına almaktı. Yer değiştirme ve ters çevirme karışımından oluşan bu algoritmaların kırılamayacağından emin olan Almanlar, şifrelerin Fransız kriptanalist George Parvin tarafından kırılmasıyla savaşta ağır yaralar almışlardır.

Bu şifreleme algoritmasında iki anahtar kullanılır. Bunlardan bir tanesi dönüşüm sırasında kullanılan matris, diğeri ise şifreleme sırasında kullanılan anahtar kelimedir. Seçilen kelimenin tekrarsız harflerden oluşmaması, alfabetik sıralamada sorun yaşanmasını engelleyecektir (URL-20).

Algoritma, Türk alfabe sistemi kullanarak şu şekilde çalışır;

- 6×6 tipinde ki matrisin satır ve sütun sayılarına ADFGVX harfleri yazılır. Bu harflerin seçilmiş olmasının sebebi mors alfabesinde kolay ayırt edilebilmesindendir.
- Rastgele yerleştirilen 29 harften arta kalan yerlere 7 adet rakam yerleştirilir ve bu rakamlarda şifreleme işleminde kullanılır.
- Şifrelenecek mesajın her harfin denk geldiği satır ve sütun harflerinden önce satır sonra sütun harfi yazılarak harf ikilileri oluşturulur.
- Tekrarsız harflerden oluşan bir anahtar kelime seçilir ve har ikilileri anahtar kelimenin altına yazılır.
- Anahtar alfabetik sıraya sokulur ve harflerin yer değişmesiyle birlikte o harflere bağlı sütunlarda yer değiştirir.
- Elde edilen yeni sütunlardaki harfler yukarıdan aşağı okunur ve şifre elde edilmiş olur.

Örnek 2.8. KARADENİZBÖLGESİ kelimesini RİZE anahtarı yardımıyla şu şekilde şifrelenir.

	A	**D**	**F**	**G**	**V**	**X**
A	E	K	İ	S	N	D
D	R	Ü	4	1	Ç	I
F	O	A	6	G	Z	T
G	Ğ	0	3	5	2	P
V	J	Ş	V	U	Y	M
X	B	F	C	Ö	L	H

Matrise harfler ve rakamlar rastgele yerleştirildikten sonra açık metini oluşturan satır ve sütun harfleri bulunur.

K	A	R	A	D	E	N	İ	Z	B	Ö	L	G	E	S	İ
AD	FD	DA	FD	AX	AA	AV	AF	FV	XA	XG	XV	FG	AA	AG	AF

Dönüştürülen harfler önce anahtar kelimenin altına sırayla yazılır.

R	**İ**	**Z**	**E**
A	D	F	D
D	A	F	D
A	X	A	A
A	V	A	F
F	V	X	A
X	G	X	V
F	G	A	A
A	G	A	F

Anahtar kelime alfabetik sıraya sokulur, yer değiştiren harflerle birlikte sütunlarda yer değiştirir.

E	İ	R	Z
D	D	A	F
D	A	D	F
A	X	A	A
F	V	A	A
A	V	F	X
V	G	X	X
A	G	F	A
F	G	A	A

Yeni tablodaki sütunlar, yukarıdan aşağı yazılır ve şifreli mesaj elde edilir. KARADENİZBÖLGESİ açık metninin şifrelenmiş hali DD AF AV AF DA XV VG GG AD AA FX FA FF AA XX AA olarak elde edilir.

Şifreleme işlemi için yapılan işlemlerin tam tersi sıraya göre yapılınca deşifreleme gerçekleşir.

2.1.2.9. Vernam Şifreleme Yöntemi

1.Dünya Savaşı'nın yaşandığı zamanlarda Amerikalılar bir mühendis olan Gilbert Vernam'ı Almanların çözemeyeceği bir şifreleme yöntemi bulması ile görevlendirmişti. Bu süreç sonunda Vernam şifresi denilen şifreleme yöntemi ortaya çıkmıştır. 1917 yılında Joseph Mauborgne, Vernam şifresinin her kullanımdan sonra anahtarın değiştirilmesinin daha güvenli hale getireceği iddiasını ortaya atmış ve tek seferlik şifre (one-time pad) ortaya çıkmıştır (Çimen vd., 2008).

Vernam şifresinde harfler ikilik tabandaki sayılarla ifade edilir. Açık metin ve mesajla aynı uzunluktaki anahtar Tablo 9'a göre ikilik tabanda yazılır. Tablo oluşturulurken o dildeki harf sayısına göre 00000 dan 11111 e kadar oluşturulur. XOR (Tablo 10) denilen işleme sokulur. Çıkan sonuçtaki rakamlar tablo 9 yardımıyla

dönüştürülüp şifreli metin elde edilir. İkilik tabanda bir sayı başka bir sayıyla iki kez XOR işlemine tutulursa sayının kendisi elde edilir.

Tablo 9. Türk alfabesinin ikilik tabanda karşılığı

Karakter	İkilik Taban	Karakter	İkilik Taban	Karakter	İkilik Taban	Karakter	İkilik Taban
A=1	00000	Ğ=9	01000	N=17	10000	U=25	11000
B=2	00001	H=10	01001	O=18	10001	Ü=26	11001
C=3	00010	I=11	01010	Ö=19	10010	V=27	11010
Ç=4	00011	İ=12	01011	P=20	10011	Y=28	11011
D=5	00100	J=13	01100	R=21	10100	Z=29	11100
E=6	00101	K=14	01101	S=22	10101	Q=30	11101
F=7	00110	L=15	01110	Ş=23	10110	W=31	11110
G=8	00111	M=16	01111	T=24	10111	X=32	11111

*Q,W,Z harfleri eklenmiştir.

Tablo 10. XOR işlemi (URL-21).

A	B	V
0	0	0
0	1	1
1	0	1
1	1	0

*Aynı rakamlar 0 farklı rakamlar 1

Örnek 2.9. ENGİN kelimesi k=YEŞİL anahtarı ile şu şekilde şifrelenir.

Kural gereği açık metinin ve k anahtarının harfleri Tablo 9 yardımıyla ikilik sisteme dönüştürülür ve XOR işlemine tabi tutulur.

E	N	G	İ	N
00101	10000	00111	01011	10000
Y	E	Ş	İ	L
11011	00101	10110	01011	01110
00101	10000	00111	01011	10000
11011	00101	10110	01011	01110
11110	10101	10001	00000	11110

XOR işleminde elde edilen ikilik tabandaki rakamlar Tablo 9 yardımıyla harf sistemine dönüştürülür ve şifreli metin bulunur.

11110	10101	10001	00000	11110
W	S	O	A	W

Şifreli metin WSOAW olarak elde edilir.

Şifreli metin, anahtar ile XOR işlemine tabi tutulursa açık metin elde edilir.

2.1.2.10. Vigenere Şifresi

Frekans analizi ile birlikte birçok şifreleme sistemi güvensiz hale gelmişti ve var olan sistemleri güvenli kılabilmek için yeni yöntemler geliştirilmeye başlanmıştı. Uzun uğraşlar neticesinde kriptograflar uzun yıllar kırılamayan ve güvenliği sağlayan yeni bir yöntem keşfettiler. Birden fazla şifre alfabenin kullanıldığı şifreleme yöntemine çok alfabeli (poli alfabetik) kripto sistemleri denmektedir (Çimen vd., 2008).

İlk olarak 1553 yılında Giovan Batista Belasa tarafından tanıtılmış olsa da 16ncı yy. da Blaise de Vigenere adlı Fransız diplomat düzenleyip geliştirmiştir.

Bu şifreleme sisteminde diğer yöntemlerin aksine açık metinde ki harfler her zaman aynı harfe dönüşmez. Anahtara bağlı olarak her harf birden fazla harfe dönüşebilir. Bunun temel nedeni döngü içinde olan birden fazla alfabe kullanılmış olmasıdır. Bu alfabelerin yer aldığı tabloya Vigenere Tablosu (Tablo 11) denilmektedir.

Vigenere kripto sisteminde düz metin m uzunluğunda ki parçalara bölünür. Seçilen m uzunluğundaki k anahtarı ile şifreleme yapıldıktan sonra m tane alfabetik karakter şifrelenmiş olur. Açık metnin ve anahtar kelimenin sayısal karşılıkları bulunur, toplanır ve o dildeki harf sayısının modu alınır. Çıkan sonucu harf sistemine çevrilerek şifreli metin bulunur.

Tablo 11. Vigenere şifreleme algoritması.

$m \in \mathbb{Z}^+$ ve $P = C = K = (\mathbb{Z}_{29})$
$k = (k_1, k_2, \ldots . k_m)$ anahtarı için
$e_k(x_1 x_2 \ldots . . x_m) = (x_1 + k_1, x_2 + k_2 \ldots . x_m + k_m)$
$d_k(y_1 y_2 \ldots . . y_m) = (y_1 - k_1, y_2 - k_2 \ldots . y_m - k_m)$

Tablo 12. Vigenere tablosu (Türk alfabe sistemine göre).

	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
A	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
B	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A
C	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B
Ç	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C
D	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç
E	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D
F	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E
G	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F
Ğ	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G
H	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ
I	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H
İ	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I
J	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ
K	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J
L	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K
M	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
N	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M
O	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N
Ö	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O
P	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö
R	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P
S	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R
Ş	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S
T	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş
U	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T
Ü	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U
V	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü
Y	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V
Z	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y

Açık metnin ilk n harfi $m_1 m_2 \dots m_n$ ve n harfli bir anahtar $k_1 k_2 \dots k_n$ olarak yazılırsa, Açık metinin tamamı, anahtar tekrarlanarak ve açık metnin karşılık geldiği anahtarın harfleriyle her seferinde $(mod\ 29)$ da toplanarak şifrelemeye çevrilir.

$m_1 + k_1 \equiv c_1 \ (mod\ 29)$

$m_2 + k_2 \equiv c_2 \ (mod\ 29)$

…….

$m_n + k_n \equiv c_n \ (mod\ 29)$

işlemlerinden sonra ortaya çıkan $(c_1\ c_2 \ldots\ldots c_n)$ şifre metnin sayı karşılığını verecektir.

Şifre çözme işlemi ise anahtarın her harfinin $(mod\ 29)$ da toplamaya göre tersi bulunarak ve şifre metnin harfleriyle toplanarak yapılır.

$c_1 + (29 - k_1) \equiv m_1 \ (mod\ 29)$

$c_2 + (29 - k_2) \equiv m_2 \ (mod\ 29)$

……..

$c_n + (29 - k_n) \equiv m_n \ (mod\ 29)$

işleminden sonra oraya çıkan $m_1 m_2 \ldots\ldots m_n$) açık metnin sayısal karşılığını verecektir (Çimen vd., 2008).

Örnek 2.10. RTEÜ anahtar sözcüğü RİZE açık metni Vigenere kripto sistemine göre şu şekilde şifrelenir.

İlk olarak anahtar kelimeden Vigerene tablosu oluşturup, harflerin kesişiminse göre şifreli metni elde etmek için;

	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
R	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	F	G	Ğ	H	I	**İ**	J	K	L	M	N	O	Ö	P
T	T	U	Ü	V	Y	Z	A	B	C	Ç	D	**E**	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş
E	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	**D**
Ü	Ü	V	Y	Z	A	**B**	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U

Şifreli metni elde etmek için üstte oluşturulan Vigenere tablosu yardımıyla açık metindeki harfler tek tek anahtardaki harflerle eşleştirme yapılır. Açık metnin satırı ile anahtar kelimenin bulunduğu sütünün kesişimin deki harf alınır.

(R) → (İ) (İ) → (E) (Z) → (D) (E) → (B)

RİZE açık metni şifrelendiğinde İEDB şifreli metni elde edilir. Bu işlem Vigenere algoritması (Tablo 11) ile şu şekilde yapılır.

RİZE açık metninin ve RTEÜ anahtarının tablo 2 yardımıyla sayısal karşılığı bulunur ve $(mod\ 29)$ a göre toplandıktan sonra tablo 2 yardımıyla yeniden karşılıkları bulunur.

Açık Metin	R	İ	Z	E
x	20	11	28	05
Anahtar	R	T	E	Ü
k	20	23	05	25
$e_k = x + k\ (mod\ 29)$	$20 + 20 \equiv 11$	$11 + 23 \equiv 05$	$28 + 05 \equiv 04$	$05 + 25 \equiv 01$
y	11	05	04	01
Şifreli Metin	İ	E	D	B

Şifreli metin İEDB olarak elde edilir. Şifreyi deşifre etmek için anahtar kelime kullanılır ve çıkarma işlemi yapılır.

Şifreli Metin	İ	E	D	B
y	11	05	04	01
Anahtar	R	T	E	Ü
k	20	23	05	25
$d_k = y - k\ (mod\ 29)$	$11 - 20 \equiv 20$	$05 - 23 \equiv 11$	$04 - 05 \equiv 28$	$01 - 25 \equiv 05$
x	20	11	28	05
Şifreli Metin	R	İ	Z	E

Vigenere şifresi, icadından yaklaşık 300 yıl sonra mucit Charles Baggage tarafından kırılmıştır. Baggage, anahtar kelimenin uzunluğunu bulmak için şifreli metindeki harf zincirini araştırmıştır (Lunde, 2009). m uzunluğundaki anahtar kelimenin sayısı n^m tanedir. Ayrıntılı inceleme neticesinde ve çeşitli tekrar örnekleriyle anahtar elde edilebilir.

2.1.2.11. Hill Şifresi

1929 yılında Lester S. Hill tarafından bulunan şifreleme yöntemi poli alfabetik bir şifreleme yöntemidir. Bu şifrelemenin mantığı, bir açık metin elemanlarının m tane parçaya bölünüp, $m \times m$ tipinde matrislerle lineer kombinasyon işlemine tutulmasıdır. Böylece bir şifreli metinden m tane alfabetik karakter üretilir.

m tane karakterden oluşan düz metin $x = x_1 x_2 \ldots . x_m$ ve şifreli metnin elemanları $y = y_1 y_2 \ldots . y_m$ olmak üzere;

$$y_1 \equiv k_{11}x_1 + k_{21}x_2 + \cdots + k_{m1}x_m \ (mod\ 29)$$
$$y_2 \equiv k_{12}x_2 + k_{22}x_2 + \cdots + k_{m2}x_m \ (mod\ 29)$$

…….

$$y_m \equiv k_{1m}x_m + k_{2m}x_2 + \cdots + k_{mm}x_m \ (mod\ 29)$$

m bilinmeyenli m tane denklemden oluşan sistem elde edilir. Bu sistemler matrislerle;

$$Y = [y_1 \quad y_2 \quad \cdots \quad y_m] \text{ ve } X = [x_1 \quad x_2 \quad \cdots \quad x_m]$$

$$K = \begin{bmatrix} k_{11} & \cdots & k_{1m} \\ \vdots & \ddots & \vdots \\ k_{1m} & \cdots & k_{mm} \end{bmatrix}_{m*m} \ (mod\ 29)$$

şeklinde gösterilir ve $Y = XK\ (mod\ 29)$ olarak ifade edilir.

Burada şifreleme ve deşifreleme fonksiyonları

$e_k(x) = XK\ (mod\ 29)$ ve $d_k(y) = YK^{-1}(mod\ 29)$

olur. k anahtar matrisi tersi alınabilen bir matris olmalıdır. Hill şifreleme algoritması tablo 13 de yer almaktadır.

Tablo 13. Hill şifreleme algoritması.

$P = C = \mathbb{Z}_{29}$
k anahtarı ve $m \times m$ tipi matrisler için
$e_k(x) = XK\ (mod\ 29)$
$d_k(x) = YK^{-1}\ (mod\ 29)$

Örnek 2.11. MERKEZİSATINALMA açık metnini $m = 4$ olacak şekilde

$K = \begin{bmatrix} 1 & -1 & 3 & 1 \\ 0 & -1 & 2 & 0 \\ -1 & 0 & 1 & -1 \\ 1 & 1 & 0 & -1 \end{bmatrix}$ anahtar matrisi ile şu şekilde şifrelenir.

Açık metin $m = 4$ olduğundan 4'erli gruplara bölünür ve tablo 2 yardımıyla sayısal değeri bulunur ve k ile işleme sokulduktan sonra $(mod\ 29)$ a göre değeri bulunur. Bulunan sonucun tablo 2 yardımıyla harf karşılığı bulunur.

$$[\text{MERK}] \rightarrow [15 \quad 05 \quad 20 \quad 13] \begin{bmatrix} 1 & -1 & 3 & 1 \\ 0 & -1 & 2 & 0 \\ -1 & 0 & 1 & -1 \\ 1 & 1 & 0 & -1 \end{bmatrix} = [08 \quad -7 \quad 75 \quad -18]$$

$$= [08 \quad 22 \quad 17 \quad 11]\ (mod\ 29) \rightarrow [\text{ĞŞOİ}]$$

$$[\text{EZİS}] \rightarrow [05 \quad 28 \quad 11 \quad 21] \begin{bmatrix} 1 & -1 & 3 & 1 \\ 0 & -1 & 2 & 0 \\ -1 & 0 & 1 & -1 \\ 1 & 1 & 0 & -1 \end{bmatrix} = [15 \quad -12 \quad 82 \quad -27]$$

$= [15 \quad 17 \quad 24 \quad 02]\ (mod\ 29) \rightarrow$ [MOUC]

$$[\text{ATIN}] \rightarrow [00 \quad 23 \quad 10 \quad 16] \begin{bmatrix} 1 & -1 & 3 & 1 \\ 0 & -1 & 2 & 0 \\ -1 & 0 & 1 & -1 \\ 1 & 1 & 0 & -1 \end{bmatrix} = [06 \quad -7 \quad 56 \quad -26]$$

$= [06 \quad 22 \quad 27 \quad 03]\ (mod\ 29) \rightarrow$ [FŞYÇ]

$$[\text{ALMA}] \rightarrow [00 \quad 14 \quad 15 \quad 00] \begin{bmatrix} 1 & -1 & 3 & 1 \\ 0 & -1 & 2 & 0 \\ -1 & 0 & 1 & -1 \\ 1 & 1 & 0 & -1 \end{bmatrix} = [-15 \quad -14 \quad 43 \quad -15]$$

$= [14 \quad 15 \quad 14 \quad 14]\ (mod\ 29) \rightarrow$ [LMLL]

Tüm 4'lü grupların karşılığı bulunduktan sonra MERKEZİSATINALMA kelimesinin şifreli hali olan ĞŞOİMOUCFŞYÇLMLL kelimesi elde edilir.

Şifreli metnin deşifre işlemine gerçekleştirmek için K^{-1} ters matrisi kullanılmak zorundadır. Öncelikle K^{-1} matrisinin bulunması gerekir.

K matrisinin tersi $K^{-1} = \begin{bmatrix} -1/4 & 3/4 & -3/4 & 1/2 \\ 1 & -2 & 1 & 0 \\ 1/2 & -1/2 & 1/2 & 0 \\ 3/4 & -5/4 & 1/4 & -1/2 \end{bmatrix}$ olur. $mod\ 29$ a göre işlem yapılırsa,

$$K^{-1} = \begin{bmatrix} 7 & 8 & 21 & 15 \\ 1 & 27 & 1 & 0 \\ 15 & 14 & 15 & 0 \\ 8 & 6 & 22 & 14 \end{bmatrix} (mod\ 29)$$ elde edilir.

Şifreli metin önce 4'erli gruplara bölünür ve K^{-1} ile işleme sokulur ve açık metin elde edilir.

$$[\text{ĞŞOİ}] \rightarrow [08 \quad 22 \quad 17 \quad 11] \begin{bmatrix} 7 & 8 & 21 & 15 \\ 1 & 27 & 1 & 0 \\ 15 & 14 & 15 & 0 \\ 8 & 6 & 22 & 14 \end{bmatrix} = [421 \quad 962 \quad 687 \quad 274]$$

$$= [15 \quad 05 \quad 20 \quad 13] \ (mod\ 29) \rightarrow [\text{MERK}]$$

Aynı işlem diğer 4'lü gruplar için de yapılır ve açık metin elde edilir.

Hill şifresi ile şifrelenmiş bir sistemi çözmek için anahtar matrise ihtiyaç vardır. $m \times m$ tipindeki bir matris için $n^{m \times m}$ tane anahtar oluşturulabilir. Bilgisayar yardımıyla ayrıntılı anahtar arama işlemi yapılabilir.

2.1.2.12. Kuvvet Fonksiyonuyla Şifreleme

Bu şifreleme yöntemi asal sayılar ve modüler aritmetiğe dayalı bir yöntemdir ve şifreleme işlemi yapılırken teorem 1.5. e göre işlem yapılır. Sistemin mantığı tablo 14 deki gibidir.

Tablo 14. Kuvvet fonksiyonu şifreleme algoritması

$p > 2$ asal sayısı ve $x, y \in \mathbb{Z}_n$ için;
$\big(e, (p-1)\big) = 1$ olacak şekilde e sayısı seçilir.
$e.d \equiv 1\ (mod\ (p-1))$ koşulunu sağlayan d sayısı seçilir.
Şifreleme fonksiyonu $e_k(x) = x^e\ (mod\ p)$ bulunur.
Deşifreleme fonksiyonu $d_k(y) = y^d\ (mod\ p)$ bulunur.

Örnek 2.12. ŞİFRELEME kelimesini tablo 15 deki harf sistemi yardımıyla kuvvet fonksiyonuna göre şu şekilde şifrelenir.

Şifreleme işlemi yapılmadan önce p, e, d sayıları oluşturulur ve tablo 15 yardımıyla açık metnin sayısal karşılığı bulunur.

Kuvvet Algoritması	İşlem
$p > 2$ asal sayısı seçilir.	$p = 41$ olsun
$\big(e,(p-1)\big) = 1$ için	$(e, 40) = 1$ için $e = 33$ olsun
$e.d \equiv 1\ (mod\ (p-1))$	$33.d \equiv 1\ (mod\ 40)$ için $d = 17$
$e_k(x) = x^e\ (mod\ p)$	$e_k(x) = x^{33}\ (mod\ 41)$
$d_k(y) = y^d\ (mod\ p)$	$d_k(y) = y^{17}\ (mod\ 41)$

Tablo 15. 41 harfden oluşan alfabe

00	A	14	L	28	Z
01	B	15	M	29	+
02	C	16	N	30	-
03	Ç	17	O	31	*
04	D	18	Ö	32	/
05	E	19	P	33	.
06	F	20	R	34	;
07	G	21	S	35	:
08	Ğ	22	Ş	36	!
09	H	23	T	37	“
10	I	24	U	38	&
11	İ	25	Ü	39	(
12	J	26	V	40	)
13	K	27	Y	41	=

Açık metnin tablo 15 yardımıyla sayısal karşılığı bulunur ve $e_k(x)$ şifreleme fonksiyonunda işleme tabi tutulur ve çıkan sonucun tablo 15 yardımıyla karşılığı bulunur.

Ş	İ	F	R	E	L	E	M	E
22	11	06	20	05	14	05	15	05

Ş için $x = 22$ $\quad e_k(22) = 22^{33}\ (mod\ 41) = 15 =$ M

İ için $x = 11$ $e_k(11) = 11^{33}\ (mod\ 41) = 34 =$;

F için $x = 06$ $e_k(06) = 06^{33}\ (mod\ 41) = 17\ =$ O

R için $x = 20$ $e_k(20) = 20^{33}\ (mod\ 41) = 36 =$!

E için $x = 05$ $e_k(05) = 05^{33}\ (mod\ 41) = 39 =$ (

L için $x = 14$ $e_k(14) = 14^{33}\ (mod\ 41) = 14 =$ L

E için $x = 05$ $e_k(05) = 05^{33}\ (mod\ 41) = 39 =$ (

M için $x = 15$ $e_k(15) = 15^{33}\ (mod\ 41) = 35 =$:

E için $x = 05$ $e_k(05) = 05^{33}\ (mod\ 41) = 39 =$ (

ŞİFRELEME açık metni $e_k(x)$ şifreleme fonksiyonu yardımıyla M;O!(L(:(şifreli mesajına dönüşür.

Şifreli metni deşifre etmek için $d_k(y)$ deşifreleme fonksiyonu kullanılır. Şifreli metnin tablo 15 yardımıyla sayısal karşılığı bulunur ve $d_k(y)$ ile işleme tabi tutulduktan sonra tablo 15 yardımıyla açık metine ulaşılır.

M için $y = 15$ $d_k(15) = 15^{17}\ (mod\ 41) = 22 =$ Ş

Şifreli metnin diğer harfleri içinde aynı işlem uygulanırsa açık metin elde edilir.

2.1.3. Asimetrik (Açık Anahtar) Şifreleme Algoritmaları

Asimetrik şifreleme yöntemlerinde simetrik şifreleme yöntemlerine nazaran en temel farkı iki ayrı anahtar kullanım esasına dayanır. Sistemde açık ve gizli olmak üzere

iki tane anahtar mevcuttur ve bu iki anahtar birbirinden farklıdır. Bu şifreleme sistemine açık anahtarlı şifreleme yöntemleri denmesinin sebebi, şifre anahtarının herkese açık olmasından kaynaklanmaktadır; Ancak şifre çözme işlemini şifrenin anahtarını bilen biri gerçekleştirir. Bu sistemde şifre anahtarına açık anahtar, deşifreleme anahtarına ise gizli anahtar denir.

Sistemin çalışma mantığı şu şekildedir (Rivest ve ark. 1978);

M=Mesaj E=Şifreleme Fonksiyonu D=Deşifreleme Fonksiyonu

1) Şifrelenmiş M mesajının şifresi çözülünce tekrar M mesajı elde edilir, yani

   $D\big(E(M)\big) = M$

   eşitliği sağlanır.
2) E ve D hesaplanması kolay olan fonksiyonlardır.
3) E fonksiyonu bilinse bile D fonksiyonunun hesaplanması için kolay bir yöntem yoktur. Yani şifreli metni sadece şifreleyen çözebilir.
4) $E\big(D(M)\big) = M$ eşitliği sağlanır.

1,2,3 şartlarını sağlayan fonksiyonlara tek yönlü kapan fonksiyon, d şartı da sağlandığında tek yönlü kapan permutasyon denir.

Açık anahtar şifreleme yöntemi için kullanılan en önemli iki yöntem DSA ve RSA yöntemleridir.

2.1.3.1. DSA Yöntemi

DSA, ilk olarak ABD tarafından kullanılmaya başlanmış olsa da, günümüzde yayın bir şekilde kullanılmaktadır. DSA, mesajları şifrelemek için kullanılmamaktadır sadece dijital imza için kullanılmaktadır.

2.1.3.2. RSA Kripto Sistemi

En ünlü açık anahtar şifreleme yöntemi olan RSA kripto sistemi asal sayılar ve modüler aritmetiğe dayanan bir yöntemdir. 1978 yılında Ron Rivest, Adi Shamir ve Leonard Adleman tarafından bulunmuştur ve isimlerinin baş harflerini vermişlerdir.

RSA şifreleme yönteminin en önemli özelliklerinden birisi asal sayıların varlığıdır. RSA şifre algoritması çalışma prensibi tablo 16 de gösterilmiştir.

Tablo 16. RSA şifreleme algoritması.

p, q asal sayı ve $x, y \in \mathbb{Z}_n$ için;
$E_k(x) = x^e \ (mod\ n)$ şifreleme fonksiyonu,
$D_k(y) = y^d \ (mod\ n)$ deşifreleme fonksiyonu olacak şekilde,
p ve q asal olacak şekilde iki asal sayı seçilir.
Mod işleminde kullanılacak n değeri hesaplanır. $n = p.q$
Euler sayısı bulunur. $\varphi\ (n) = (p-1)(q-1)$
$1 < e < \varphi\ (n)$ için $(\varphi\ (n), e) = 1$ olacak şekilde e değeri bulunur.
Şifreleme anahtarı (e, n) oluşturulur.
Şifreleme fonksiyonu $E_{e,n}\ (x) = x^e\ (mod\ n)$ oluşturulur.
$1 < d < \varphi\ (n)$ ve $(e.d) \equiv 1 (mod\ \varphi\ (n))$ olacak şekilde d değeri bulunur.
Deşifreleme anahtarı (d, n) oluşturulur.
Deşifreleme fonksiyonu $D_{d,n}\ (y) = y^d\ (mod\ n)$ oluşturulur.

*n, e ilan edilirken p,q,d gizli tutulur.

Seçilen p ve q asal sayıları ne kadar büyük seçilirse asal çarpanlara ayrılması o kadar zor olur ve şifrenin kırılması o kadar zorlaşır. Günümüzde bilgisayarlar bile çok büyük asal sayıları çarpanlara ayırmakta zorlanmaktadır.

353246193440277012127260497819846436867119740019762502364930346877612125367942320005854795652808834 99

Şekil 11. Yüz basamaklı bir asal sayı (Küçük vd., 2013)

Örnek 2.13. **“**VERÇENİK” M mesajı $p = 7$ ve $q = 11$ olacak şekilde tablo 17 deki alfabe ile RSA yöntemi ile şu şekilde şifrelenir.

RSA Şifre Algoritması	İşlem
p ve q asal sayıları	$p = 7$ ve $q = 11$
$n = p.q$	$n = 7.11 = 77$
$\varphi\,(n) = (p-1)(q-1)$	$\varphi\,(n) = 6.10 = 60$
$\big(e, \varphi\,(n)\big) = 1 \quad (1 < e < \varphi\,(n))$	$e = 13 \;\; (1 < 13 < 60)$ ve $(13{,}60) = 1$
$k = e, n$	$k = 13{,}77$
$E_k(x) = x^e \;(mod\; n)$	$E_{13,77}(x) = x^{13} \;(mod\; 77)$
$(e.d) \equiv 1(mod\; \varphi\,(n)) \;\; (1 < d < \varphi\,(n))$	$(13.37) \equiv 1(mod\; 60) \;\; (1 < 37 < 60)$
$k = d, n$	$k = 37{,}77$
$D_k(y) = y^d \;(mod\; n)$	$D_{37,77}(y) = y^{37} \;(mod\; 77)$

Tablo 17. 77 harften oluşan alfabe.

00	A	26	V	52	[
01	B	27	Y	53	Ώ
02	C	28	Z	54	€
03	Ç	29	Q	55	∏
04	D	30	X	56	∑
05	E	31	W	57	₳
06	F	32	.	58	₭
07	G	33	,	59	@
08	Ğ	34	:	60	©
09	H	35	;	61	®
10	I	36	“	62	Æ
11	İ	37	!	63	Ħ
12	J	38	£	64	ɓ
13	K	39	^	65	ƈ
14	L	40	$	66	Ǿ
15	M	41	%	67	ȸ
16	N	42	&	68	ᵩ
17	O	43	/	69	ɸ
18	Ö	44	(	70	<
19	P	45	)	71	>
20	R	46	=	72	∧
21	S	47	+	73	И
22	Ş	48	-	74	Ѭ
23	T	49	*	75	Г
24	U	50	?	76	Ψ
25	Ü	51	]	77	ȣ

M mesajının tablo 17 yardımıyla sayısal karşılığı bulunur ve şifreleme fonksiyonu $E_{13,77}(x) = x^{13}\ (mod\ 77)$ de işleme sokulur. Çıkan sonucun karşılığı tablo 17 yardımıyla harfe dönüştürülür..

(V)→ (26) için $x = 26,\ \ E_{13,77}(26) = 26^{13}\ (mod\ 77) = 75 =$ Γ

(E)→ (05) için $x = 05,\ \ E_{13,77}(05) = 05^{13}\ (mod\ 77) = 26 =$ V

(R)→ (20) için $x = 20,\ \ E_{13,77}(20) = 20^{13}\ (mod\ 77) = 69 =$ ϕ

(Ç)→ (03) için $x = 03,\ \ E_{13,77}(03) = 03^{13}\ (mod\ 77) = 38 =$ £

(E)→ (05) için $x = 05,\ \ E_{13,77}(05) = 05^{13}\ (mod\ 77) = 26 =$ V

(N)→ (16) için $x = 16,\ \ E_{13,77}(16) = 16^{13}\ (mod\ 77) = 37 =$!

(İ)→ (11) için $x = 11,\ \ E_{13,77}(11) = 11^{13}\ (mod\ 77) = 11 =$ İ

(K)→ (13) için $x = 13,\ \ E_{13,77}(13) = 13^{13}\ (mod\ 77) = 41 =$ %

M mesajı $E_{13,77}(x) = x^{13}\ (mod\ 77)$ şifreleme fonksiyonu yardımıyla ΓVϕ£V!%İ şifreli metnine dönüşür. Şifreli metin herkese açıktır ve herkes rahatlıkla ulaşabilir.

Deşifreleme işlemi yapmak için $D_{37,77}(y) = y^{37}\ (mod\ 77)$ deşifreleme fonksiyonunu kullanmak gereklidir. Deşifreleme işlemini ancak fonksiyonu bilen kişi gerçekleştirebilir. Şifreleme işlemindeki işlemlerin aynısı yapılır.

(Γ)→ (75) için $D_{37,77}(75) = 75^{37}\ (mod\ 77) = 26 =$ V

Elde edilen sonuçlar tablo 17 den harf karşılığı bulunur ve M mesajına ulaşılır.

2.1.4. Simetrik ve Asimetrik Şifrelemelerin Genel Özellikleri

Simetrik ve asimetrik şifre algoritmaları arasındaki farklar ve genel özellikleri tablo 18 deki gibidir.

Tablo 18. Simetrik ve asimetrik şifreleme algoritmaları arasındaki farklar

Simetrik Şifreleme Algoritmaları	Asimetrik Şifreleme Algoritmaları
Anahtar, hem şifrelemede hem de deşifreleme işleminde kullanılır.	Şifreleme ve şifre çözmek için farklı anahtarlar kullanılır.
Gönderici ve şifre çözücü aynı algoritma ve aynı anahtarı kullanılır.	Gönderici alıcının açık anahtarını bilmelidir. Gönderici ile alıcının anahtarı farklıdır.
Şifreleme için kullanılan algoritma gizli tutulmalıdır.	Şifreleme algoritması açık, deşifreleme algoritması gizli olmalıdır.
Diğer algoritmalara göre hızlı çalışır.	Şifreler uzun ve büyük olduğundan genelde yavaş çalışır.

2.2. Kriptanaliz

Kriptanaliz, açık metni elde etme veya anahtarı elde etme bilimidir. Yani şifreli metinlerin şifrelerinin kırılması işlemidir. Başka bir deyişle kriptanaliz; sistemi analiz etmek, güçlü ve zayıf yanlarını test etmek için kullanılacağı gibi, üçüncü şahısların şifreyi kırıp açık metne ulaşmaları amacıyla da kullanılabilir.

Kripto-analizci, şifreleme algoritmasının bütün detaylarına ulaşma yeteneğine sahiptir ve sistemde sadece anahtar gizlidir (Menezes vd., 1997). Analizcinin amacı herhangi bir algoritma kullanarak şifreli metinlerin açık halini elde etmektir.

Bir kripto sisteminin açık metnini elde edebilmek için dört yaygın model vardır. (Sakallı, 2006).

- *Sadece şifreli metin saldırısı:* Analizcinin, şifreli metini bildiği varsayılan saldırılardır.
- *Bilinen açık metin saldırısı:* Analizcinin, açık metni ve ona karşılık gelen şifreli metni bildiğini varsayılan saldırılardır.
- *Seçilmiş açık metin saldırısı:* Analizcinin, şifreleme algoritmasını bildiği varsayılan saldırılardır. Bu durumda açık metin ve şifreli metin elde edilebilir.
- *Seçilmiş şifreli metin saldırısı:* Analizcinin, deşifreleme algoritmasını bildiği varsayılan saldırılardır. Bu durumda şifreli metin ve açık metin elde edilebilir.

Belli başlı kriptanaliz yöntemleri şunlardır.

2.2.1. Doğrusal Kriptanaliz

1993 yılında Matsui tarafından DES algoritmalarına kriptanalitik bir saldırı tipi olarak keşfedilmiştir. Saldırganın algoritmayı bildiği ve belli sayıda açık metin ve şifreli metne sahip olduğu varsayılır (Matsui, 1993).

2.2.2. Diferansiyel Kriptanaliz

1991 yılında Biham tarafından keşfedilmiştir. Bu kriptanaliz yöntemi açık metin ikilileri farkının bunlara karşılık gelen şifreli metin ikilileri üzerindeki etkisini kullanarak analiz yapar (Bilham vd., 1991).

Bu iki yöntemin dışında imkânsız diferansiyel kriptanaliz, çoklu set saldırıları, interpolason saldırısı, boomerang saldırısı, kare saldırısı gibi çeşitli yöntemler de mevcuttur.

3. TARTIŞMA VE SONUÇLAR

Kriptoloji, bireylerin ve toplumların kendilerine ait bilgileri yabancı gözlerden saklamak için ortaya çıkmış, içinde matematiği barındıran bir bilim dalıdır. Bu çalışmada daha çok şifreleme biliminin matematiksel yöntemlerle olan ilişkisini incelemiş olsak da, günümüzde askeri alanın dışında gelişen teknoloji ile birlikte cep telefonlarında, kredi kartlarında, şifreli kanallarda, internet üzerinde yapılan sanal alışverişler ve daha birçok konuda kriptolojiden faydalanılmaktadır. Bu sayede gündelik hayatımızda kullandığımız, hayatımızı kolaylaştıran birçok şeyde farkında olmasak bile kriptolojinin etkisi görülmektedir.

Bu tez çalışması sırasında geçmişten günümüze kadar kullanılan temel şifreleme yöntemleri incelenmiştir ve örneklerle açıklanmaya çalışılmıştır. Bazı yöntemlerin ne denli kolay bazılarınınsa seçilecek rakamlara göre ne kadar zor olabileceği gözlemlenmiştir. Şifreleme tekniklerinden hangisini kullanacağımızı biz belirlesek de, anahtar ne kadar büyükse sistem de o kadar güvenli bir hal alacaktır. Ayrıca ülkemizdeki bu alanda yapılan çalışmaların yeni yeni ortaya çıktığı görülmüştür.

Geçmişten beri kırılamaz denilen şifrelerin kırılması ile yeni algoritma çalışmalarının yapılmasını, yeni şifrelerin bulunmasını sağlamaktadır. Kriptograflar yeni şifreler üretirken, kriptananalistler de bu şifreleri kırmak için çalışmaktadırlar. Bu rekabet ve matematiğin sayesinde gelecekte bizi yeni yöntemler, yeni algoritmalar beklemektedir.

4.ÖNERİLER

Kriptolojinin önemi her geçen gün artmaktadır ve bu bilimle uğraşan sayısında bir artış gözlemlenmektedir. Ancak her işte olduğu gibi nitelikli ve donanımlı bireylerin yetişebilmesi için, kriptoloji, bilgi güvenliği, sistem güvenliği, yazılım gibi konuların temelleri küçük yaşlardan itibaren atılmalıdır. Özellikle üniversitelerin matematik ve bilgisayar mühendisliği bölümlerinde kriptoloji bilimi zorunlu ders olarak okutulmalıdır. Kriptoloji kurslarının açılması teşvik edilmelidir.

En güvenilir sistemlerin çözüldüğü, kırılamaz denilen şifrelerin kırıldığı günümüzde farklı algoritmalar geliştirilmeli ve var olanların güvenlik derecesi artırılmalıdır. Ulusal bilgilerimizi, ulusal yazılımlarımızı kendi ulusal şifreleme programlarımızla yapmak için, ülke olarak kendi milli kriptolarımızı yazılımlarımızı geliştirmeliyiz.

KAYNAKLAR

Altindiş, H., 2011. Sayılar Teorisi ve Uygulamaları. Erciyes Üniversitesi Yayınları, 3. Baskı, 978-975-9703-60-8, 308 s.

Arslan, G., 2009. Kriptoloji Kavramları ve Kriptoloji Analiz Merkezi, UEKAE.

Aslan, B., 2013. Blok Şifreler İçin Cebirsel İkili Doğrusal Dönüşüm Tasarımı ve Modern Bir Blok Şifreye Uygulanması. Doktora Tezi. Trakya Üniversitesi. Fen Bilimleri Enstitüsü, Edirne, Türkiye, 153 s.

Balcı, M., 2010. Matematik Analiz 1. Balcı Yayınları, 8. Baskı, 975-668-302-6, 341 s.

Bilgiç, H., 2014. Soyut Cebir Ders Notları, 110 s.

Bilham, E. Ve Shamir, A., 1991. Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology . 1. Baskı, 105 s.

Çallıalp, F., 2011. Örneklerle Soyut Cebir. Birsen Yayınevi, Genişletilmiş Baskı, 975-511-350-9, 343 s.

Çeşmeci, Ü., 2009. Kriptoloji Tarihi. UEKAE Dergisi, 1, 21-29.

Çimen, C., Akleylek, S. ve Akyıldız E., 2008. Şifrelerin Matematiği: Kriptografi. 1 ODTÜ Yayıncılık, 3. Baskı, 131 s. 8-9-18-19-20-29-33-34-35-40-41-3- 58-68-73-74-116

Erdoğan, M., ve Yılmaz, G., 2008. Çözümlü Problemlerle Soyut Cebir ve Sayılar Teorisi. Beykent Üniversitesi Yayınevi, 1. Baskı, 978-975-6319-02-4, 261 s.

Erhan, M., 1993. RSA Algoritmasını Kullanan Şifreleme/Deşifreleme Yazılımının Tasarımı. Yüksek Lisans Tezi. İstanbul Teknik Üniversitesi. Fen Bilimleri Enstitüsü İstanbul, Türkiye, 83 s.

Gül, S., 1997. RSA Tabanlı Halka Açık Anahtarlı Kriptosisteminin Uygulanması. Yüksek Lisans Tezi. Ortadoğu Teknik Üniversitesi. Fen Bilimleri Enstitüsü, Ankara, 56 s.

Hassanpour, A., 2015. Asal Sayıların Şifreleme Teorisindeki Uygulamaları. Yüksek Lisans Tezi. Atatürk Üniversitesi. Fen Bilimleri Enstitüsü, Erzurum, Türkiye, 85 s.

Kahn,D., 1996. The Codebreakers. The Macmilian Company, 473 s. 71-77-82-83-243

Karaahmetoğlu, O., 2010. Gizli Anahtarlı Kriptosistemlerin Tasarımında Cebirsel Yapıların Önemi Ve Kriptanaliz. Doktora Tezi. Trakya Üniversitesi. Fen Bilimleri Enstitüsü, Edirne, Türkiye, 243 s.

Kodaz, H., ve Botsalı, F. M., 2010. Simetrik ve Asimetrik şifreleme Algoritmalarının Karşılaştırılması, Selçuk Üniversitesi Teknik Bilimler Meslek Yüksekokulu Teknik - Online Dergi, 9, 10-23.

Küçük, Y., Dereli, Y., Büyükköroğlu, T., Erdoğan, N.K., Akyar,E., Mutlu, F., Cafer, V., 2013. Matematik-II. Saray Matbaacılık, 2. Baskı, 978-975-06-1493-4, 206 s. 170

Külen, F., 2013. Kriptolojide Bazı Şifreleme Yöntemlerinde Cebirsel Yaklaşımlar. Yüksek Lisans Tezi. Gaziosmanpaşa Üniversitesi. Fen Bilimleri Enstitüsü, Tokat Türkiye, 45 s. 17.

Lunde, P., 2009. Şifreler kitabı. NTV Yayınları, 1. Baskı, 978-605*5813-18-5, 279 s., Akın, D. (Ç.), 105.

Matsui, M., 1993. Linear Cryptanalysis Method for DES Cipher, in Advances in Cryptology–EUROCRYPT. 1. Baskı, 397 s.

Menezes, A.J., Oorschot, P.C. and Vanstone, S.A., 1997. Handbook of Applied Cryptography Chapter. CRC Press, USA.

Öztürkmenoğlu, Ş., 2016. Matrislerle Şifreleme Üzerine. Yüksek Lisans Tezi. Sıtkı Kocaman Üniversitesi. Fen Bilimleri Enstitüsü, Muğla, Türkiye, 64 s.

Rivest, R., Shamir, A. and Adleman,L.,1978. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM,120-126

Sakallı,M.T., 2006. Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi. Doktora Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne, 203 s.

Şiap, V., 2008. Matris Kodlar İle Mceliece Şifreleme Sistemi. Yüksek Lisans Tezi. Sakarya Üniversitesi. Fen Bilimleri Enstitüsü, Sakarya,Türkiye, 85 s.

Soyalıç, S., 2005. Kriptografik Hash fonksiyonları ve uygulamaları. Yüksek Lisans Tezi. Erciyes Üniversitesi. Fen Bilimleri Enstitüsü, Kayseri, Türkiye, 92 s.

Stinson, D.R., 2006. Cryptograhy Theory and Practıse. Taylor & Francis Group, LLC, 593 s. 3-5-7

URL-1, 2016. http://www.isa-sari.com/rosetta-tasi-ve-misir-hiyerogliflerinin-cozumu/ (18 Ocak 2016)

URL-2, 2016. https://en.wikipedia.org/wiki/Scytale (25 Ocak 2016)

URL-3, 2016. http://www.wseas.us/e-library/conferences/2011/Cambridge/ NEHIPISIC /NEHIPISIC-20.pdf (28 Nisan 2016)

URL-4, 2016. http://www.bilinmeyenler.org/voynich-el-yazmasi.html (27 Ocak 2016)

URL-5, 2016. https://en.wikipedia.org/wiki/Jefferson_disk (30 Ocak 2016)

URL-6,2016. http://www.acikbilim.bom/2014/11/dosyalar/kriptoloji-tarihine_yolculuk-turler-ornekler.html (02 Şubat 2016)

URL-7, 2016. http://e-bergi.com/y/enigma (23 Nisan 2016)

URL-8, 2016. https://recepsatir.wordpress.com/category/kriptoloji/ (23 Nisan 2016)

URL-9, 2016. http://bilgimat.com/ilk-bilgisayar-ve-bilgisayarin-tarihcesi/ (23 Nisan 2016)

URL-10, 2016. http://bilgisayarkavramlari.sadievrenseker.com/2009/06/11/idea_ulus lararasi -sifreleme-algoritmasi/ (23Nisan 2016)

URL-11, 2016. http://enethaberci.com/sondakika-guncel-haberleri/ayse-tatile-cikali-tam-36-yil-oldu-45838.html) (23 Nisan 2016).

URL-12, 2016. http://www.ssm.gov.tr/katalog2007/data/397/uruntr/18.htm (23 Nisan 2016).

URL-13, 2016. https://www.cyber-warrior.org/forum/kriptoloji-hakkinda-odev-_sunu mu -sau_461693,1.cwx&get=last. (22 Şubat 2016)

URL-14, 2016. http://docplayer.biz.tr/1146665-Sifreleme-bilimi-prof-dr-seref-_sagirog lu-gazi-universitesi-muhendislik-fakultesi-bilgisayar-muhendisligi-bolumu-malte pe-ankara.html (05 Mart 2016)

URL-15, 2016. https://tr.wikipedia.org/wiki/Sezar_%C5%9Fifrelemesi (24 Nisan 2016)

URL-16, 2016. https://en.wikipedia.org/wiki/Bifid_cipher (24 Nisan 2016)

URL-17, 2016. https://en.wikipedia.org/wiki/Trifid_cipher (25 Nisan 2016)

URL-18, 2016. http://www.wseas.us/e-library/ conferences/ 2011/Cambridge/ NEHIPI SIC / NEHIPISIC-20.pdf (28 Nisan 2016)

URL-19, 2016. http://www.hakkindabilginedir2016.com/mors-alfabesi-nedir-15501. Aspx (01 Nisan 2016)

URL-20, 2016. http://bilgisayarkavramlari.sadievrenseker.com /2010/06/ 07/adfgvx-sifrelemesi/ (29 Nisan 2016)

URL-21, 2016. https://tr.wikipedia.org/wiki/XOR_kap%C4%B1s%C4%B1 (01 Mayıs 2016)

Wenbo, M., 2003. Modern Cryptograhy. Prentice Hall PTR, 0-13-06643-1, 648 s.

Yılmaz, S. ve Salcan, O., 2008. Siber Uzayda Güvenlik ve Türkiye. Milenyum Yayıncılık,113-117

ÖZGEÇMİŞ

Engin YEŞİLBAŞ, 08.03.1985 yılında Rize Pazar'da doğdu. İlköğretimini 1991 yılında başladığı Derebaşı Köyü İlköğretim Okulunda, Ortaöğrenimini ve Liseyi 2002 yılında Pazar 75. Yıl İ.M.K.B. Anadolu Lisesinde tamamladı. 2003 yılında başladığı Gaziantep Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümünü 2010 yılında bitirdi. 2013 yılında Recep Tayyip Erdoğan Üniversitesi Fen Bilimleri Enstitüsü Matematik Bölümün'de başladığı yüksek lisans eğitimini devam ettirmektedir. 2012-2013 yılları arasında Rize İl Sağlık Müdürlüğüne görev yapmış olup, 2013 yılından itibaren Rize Kamu Hastaneler Birliği Genel Sekreterliği Merkezi Satınalma Biriminde ki görevine devam etmektedir. Engin YEŞİLBAŞ, orta seviye İngilizce bilmektedir.