BİLGİ GÜVENLİĞİ DERSİ
5. HAFTA

KRİPTOGRAFİ'YE GİRİŞ

Kriptoloji, Kriptografi ve Kripto Analiz

Kriptoloji, kriptografi ve kripto analiz olmak üzere iki ana dalı içeren, şifreli yazıların incelenmesiyle ilgilenen bilimsel çalışma alanıdır. Yani kriptoloji, hem kriptografiyi hem de kripto analizi kapsar ve bu alandaki genel çalışmaların adıdır.

Kriptoloji, Kriptografi ve Kripto Analiz

Kriptografi, mesajların güvenli bir şekilde iletilmesi için şifreleme yöntemleri geliştiren ve uygulayan bilim dalıdır. Başka bir deyişle, bilgilerin yetkisiz erişimlere karşı korunması için bu bilgileri okunamaz hale getirme sanatı ve bilimidir. Kriptografi, sadece metinlerin değil, her türlü verinin şifrelenmesi ile ilgilidir.

Kriptoloji, Kriptografi ve Kripto Analiz

Kripto analiz, şifrelenmiş mesajların, orijinal (şifresiz) hallerine dönüştürülmesi için yapılan çalışmaları ifade eder. Bu, şifrelerin güvenliğini test etme, zayıflıklarını bulma ve gerektiğinde şifreleri kırmaya çalışma işlemidir.

Kriptografi

Kriptografi, Kripto (gizli) ve Grafi (yazmak) kelimelerinin birleşiminden oluşan ve üçüncü şahısların mesajları ele geçirme tehdidi altında güvenli haberleşme yöntemlerini ve uygulamalarını araştıran interdisipliner bir bilim dalıdır.

Kriptografinin Temel Uygulama Alanları

- Elektronik **Ticaret**
- Kartlı Ödeme Sistemleri
- Dijital Paralar
- Bilgisayar Ağları
- **Askeri Haberleşme**

Kriptografinin İlgi Alanları

Yazının icadından günümüze kadar evrilen kriptografi bilimi aşağıdaki problemlerle ilgilenir:

- İki taraflı ve çok taraflı güvenli haberleşme problemi
- Anahtar üretme problemi
- Gizli bilginin paylaşılması problemi
- Şifrelenmiş bilgiyi çözmeden üzerinde işlem yapma problemi
- Sayısal imza problemi
- Uzaktan rastsal sayı seçme problemi
- Veri bütünlüğü problemi

Klasik Dönem Kriptografik Algoritmalar

- Yazının M.Ö. 3000li yıllarda Sümerler tarafından icat edilmesinden günümüze insanlığın en temel sorunlarından biri güvenli haberleşme olagelmiştir. Bilinen en eski kriptografik obje Irakta keşfediler 1600 yıllara ait bir toprak küp olarak tarihe geçmiştir.

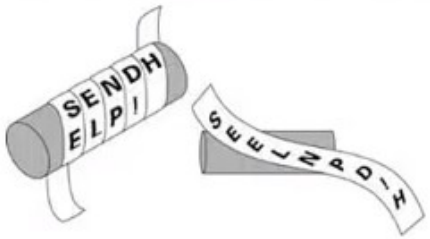
- Antik Çin ve Mısırda mesajlar grafik imgelere dönüştürülerek bilgi korunmaya çalışılıyordu.
- Hint medeniyetinde ise kelimelerin ilk harfleri sona taşınarak ‘ay’ kelimesi eklenerek mesajlar güvenli hale getirilmesine çalışılıyordu.

SCYTALE Kriptografi Yöntemi

M.Ö. 700'lü yıllarda Spartalılar askeri haberleşmede transpozisyona dayalı şifreler kullanıyordu. SCYTALE adlı sopalara sarılan şeritlere mesaj yazılıyor ve açık şerit metni üzerinde görenler anlamlandıramıyorlardı.

Mesaj: 

YARIN SABAH GELIYORLAR HAZIRLANIN



YIAHLOAARN

Anahtar: Sopanın Çapı ANBGIRRZLI

RSAEYLHIAN

SCYTALE Kriptografi Yöntemi

Transpozisyon, şifreleme işlemi sırasında metin bloklarının yerlerini değiştirerek şifreleme yapar. Bu işlem, harf yer değiştirme, satır yer değiştirme veya sütun yer değiştirme gibi yöntemlerle gerçekleştirilebilir.

ATBAŞ Alfabesi

M.Ö. 600'lü yıllarda İbranicede atbaş adlı alfabenin son harfiyle ilk harfinin yer değiştirilmesine dayalı bir şifreleme yöntemi kullanılmıştır.

Mesaj: MERHABA NASILSIN

NVISZYZ MZHROHRM

Sezar Şifreleme

M.Ö. 100'lü yıllarda Roma imparatoru Julius Sezar'ın güvenli haberleşme için kullandığı monoalfabetik Sezar Şifrelemesi alfabenin anahtar kabul edilen 3 sayısı kadar kaydırılarak karakterlerin yerdeğişimine dayanıyordu.

Örneğin Anahtar K=3 için Mesaj: Merhaba 

JBOEXYX olur.

Mesaj şifrelenirken alfabe tek ve sabit olduğundan bu tip şifreleme algoritmalarına **monoalfabetik** denir.

Klasik Kriptografi

- M.S. 8.yy'da Basralı Abdürrahman El-Halili'nin Kitab-ül Muamma adlı eserinde gizli mesajlaşmalar için permütasyon ve kombinasyon hesaplamalarını anlatır.
- 9.yy'da Arap matematikçi Ebu Yusuf El-Kindi 'Şifreli Mesajların Çözülmesi' adlı
- eserinde bilinen ilk sistematik kriptoanaliz yöntemi olan **frekans analizi** yöntemini
- anlatmıştır.

- 12.yy'da Musullu İbn-i Adlan, frekans analizi yöntemi için gerekli olan örnek sayılarını hesaplamayı geliştirmiştir.

Kriptografide Frekans Analizi

Kriptografide frekans analizi, bir şifreli metindeki karakterlerin (genellikle harflerin) tekrar etme sıklıklarını inceleyerek şifreyi çözmeye çalışan bir yöntemdir.

Bu teknik, bir dildeki harfler, sayılar veya diğer karakterlerin kullanım sıklıklarının tutarlı bir şekilde farklılık göstermesine dayanır. Örneğin, İngilizce'de "e" harfi en sık kullanılan harfken, "z" harfi çok daha az kullanılır. Frekans analizi, bu tür istatistiksel bilgileri kullanarak şifreli metinlerdeki harflerin gerçek eşleşmelerini tahmin etmeye çalışır.

Frekans Analizinin Adımları

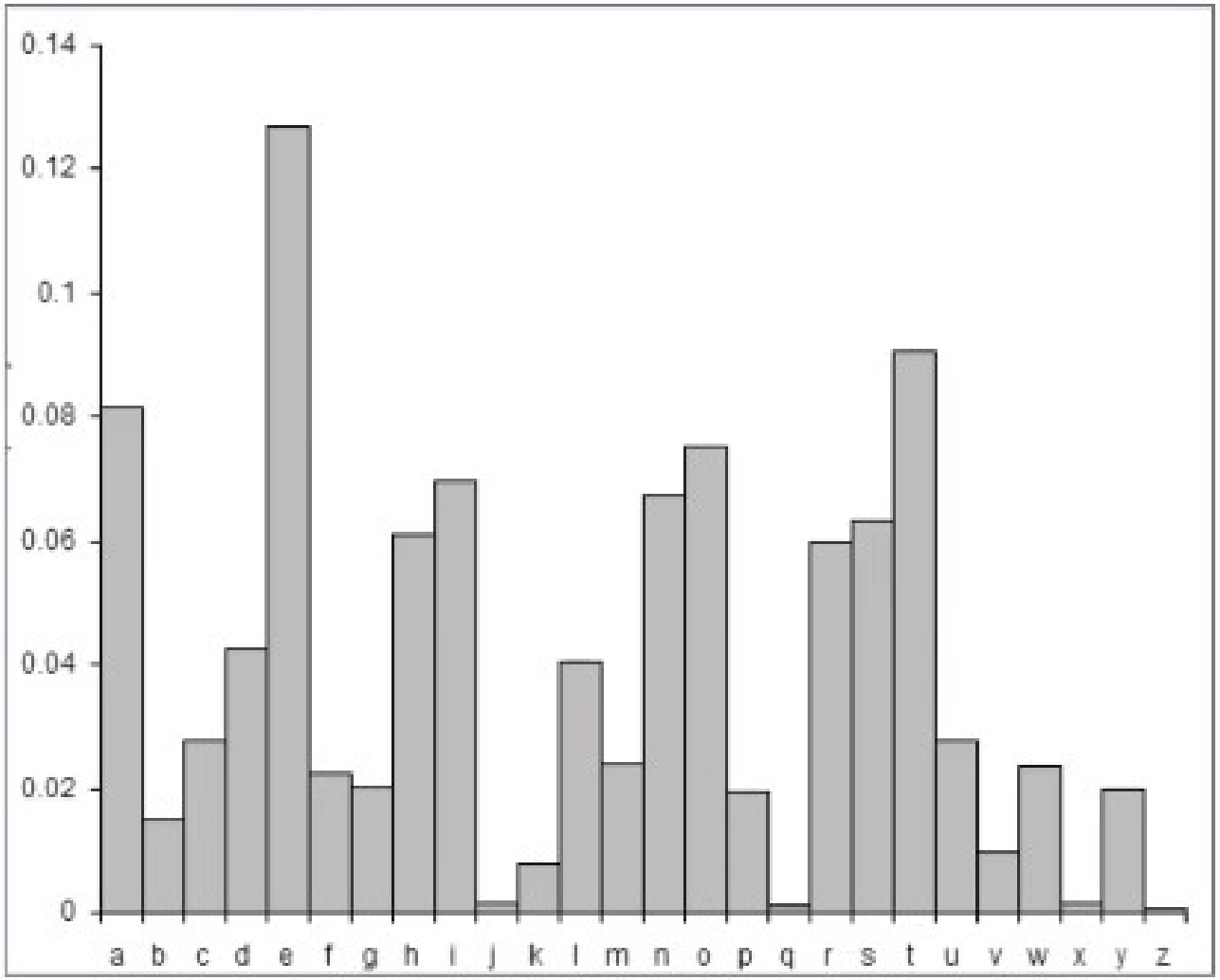
Veri Toplama: Şifreli metindeki her bir karakterin ne kadar sık geçtiğini sayma işlemi yapılır. Bu, harfler, rakamlar veya diğer semboller olabilir.

Frekans Dağılımının Analizi: Elde edilen frekans dağılımı, dilin bilinen karakter frekansı ile karşılaştırılır. Örneğin, eğer bir metinde en çok geçen harf "X" ise ve biliniyorsa ki İngilizce'de en sık kullanılan harf "E" ise, analiz yapan kişi "X" harfinin şifreli metinde "E"yi temsil ettiğini tahmin edebilir.

Hipotez Testi ve Ayarlama: İlk tahminler yapılıp bazı harflerin şifresi çözüldükten sonra, analist metnin geri kalanını çözmek için bu bilgileri kullanır. Bu süreç, metnin okunabilir hale gelene kadar devam eder.

Frekans Analizi Görsel

Not: Klasik kriptografide bir metni mono alfabetik algoritmalar ile şifrelediğimiz zaman kelimelerin yeri değişebilir ama tekrar etme sıklığı değişmez!!!



İlk Kırılma: Poli Alfabetik Algoritma

- 14.yy'da El-Kalkeşandi ilk polialfabetik şifreleme algoritmasını İbn el-Durayhim'in
- önceki bilimsel çalışmalarına dayanarak eserlerinde anlatmıştır.
- 16.yy'da ilk Giovan B. Bellaso tarafından geliştirilen 'kırılamaz şifre', adını
- diplomat Blaise de Vigenère'den alacaktır.
- Polialfabetik şifrelemede bir sembolün birden fazla karşılığı olabildiği için kırılma
- ları monoalfabetik algoritmalara göre daha zordur.
- Vigenère'de her harfin şifrelemesi için ayrı bir alfabe kullanıldığından polialfabetik
- bir algoritmadır. 19.yyda Charles Babbage tarafından kırılmıştır.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tabula Recta

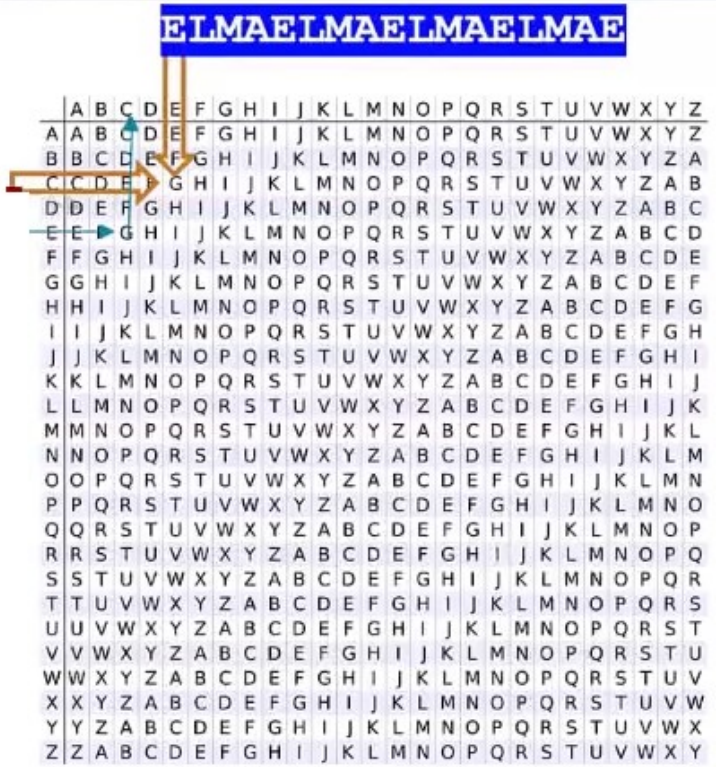
Vigenére Şifreleme

Örnek: **Mesaj**: COVID NE ZAMAN BITER, **Anahtar**: ELMA

bu mesajın uzunluğu kadar seçilen anahtar kelime tekrarlanır.

COVIDNEZAMANBITER
ELMAELMAELMAELMAE
GZHIHYQZEXMNFTFEV

C-E ile eşleştiği için tabloda C satırı ve E sütününa karşı gelen sembol yazılır yani G. Bu şekilde mesajdaki her harf anahtarın karşı gelen harfi ile işlenerek şifreleme tamamlanır. Şifre çözerken anahtardaki sembole Karşı gelen satırdan şifreli harfe kadar gidilir ve sütundaki karşıgelen harf ile çözülür.



SORU

Klasik dönemdeki kriptografi algoritmalarında boşluk karakteri ya da rakamlar da şifreleniyor muydu?

Bunların şifrelenmesi için nasıl bir yol izleniyordu?

Klasik algoritmalarda boşluk ve rakamlar çoğunlukla şifrelenmezdi.

Şifrelenmek istenirse genişletilmiş alfabe, sembol ataması ya da özel kurallar eklenerek işlenirdi.

Şimdi Sıra Sizde

Vigenére Algoritmasını kullanarak **Merhaba** kelimesini şifreleyiniz. Anahtar: **Su**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Şimdi Sıra Sizde

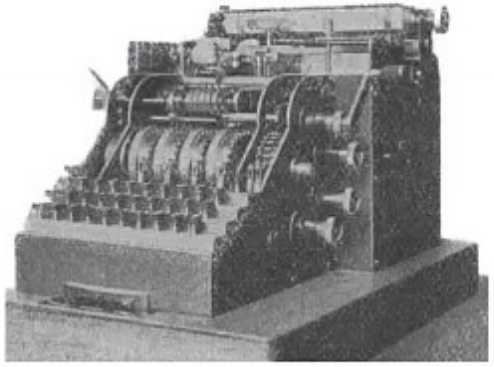
BILGI GUVENLIGI kelimesini şifreleyiniz. Anahtar: **BST**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

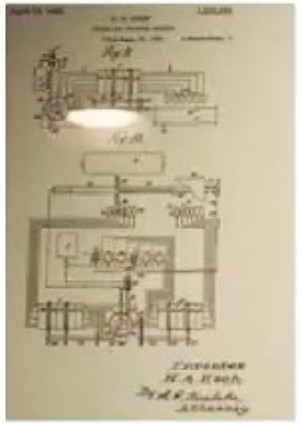
Modern Dönem Kriptografi Uygulamaları

1917'de Vernam tarafından telgraf güvenliği için geliştirilen aygıt, kırılması imkansız olan One Time Pad şifreleme yöntemini kullanıyordu. Bu teknikte her mesaj yalnızca bir defalık anahtarla şifreleniyordu. Ancak mesaj uzunluğu kadar anahtar gerekliydi, uygulamada gereken bu çok uzun anahtarlar sorun teşkil ediyordu. Bu dönemde ilk rotorlu kriptografik elektromekanik cihazlar ortaya çıktı.

Edward Hebern
ABD 1917



Arthur Scherbius
Almanva 1918



Hugo Koch
Hollanda 1919

Arvid Damm
İsveç 1919

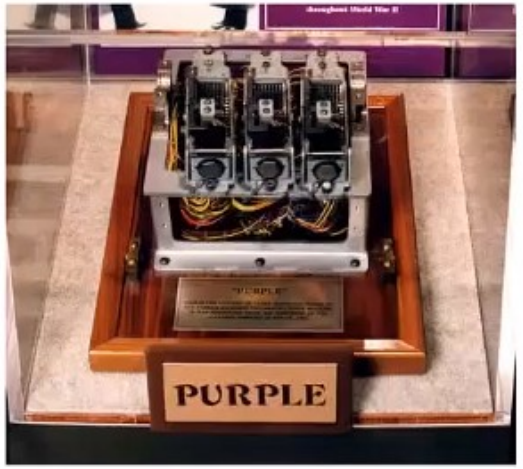
Modern Dönem Kriptografi Uygulamaları

2. Dünya savaşının kaderini kriptografi belirledi. Alman Enigma şifreleme aygıtının İngiliz Alan Turing'in ekibi ve Japon Purple şifreleme cihazının Amerikan Williem Friedman'ın ekibi tarafından kırılması savaşın gidişatını müttefikler lehine değiştirmiştir.

Arthur Scherbius

Alan Turing

Kazuo Tanabe



William Friedman

2. Dünya savaşının ardından ekonominin stratejik gücünü keşfeden ABD, sivil ve ticari uygulamalar için kriptografinin kullanımının önünü açmıştır.

Modern Dönem Kriptografi Algoritmalar

- Kerckhoff prensibi uyarınca algoritmaların saldırgan tarafından bilindiği varsayımıyla tasarlanması gerekir.
- Geçmişte güvenli kabul edilen pek çok algoritma bilişim teknolojilerindeki ilerlemeler sonucu bugün kırılmıştır.
- Modern kriptografide güvenlik paradigması şifreleme algoritmalarının gizliliğinden şifreleme anahtarlarının gizliliğine kaymıştır. Gizli olan **anahtarların korunması** için özel 'kasalara' ve **dağıtımları** için de güvenli yöntemlere ihtiyaç duyulur.
- Anahtar uzunluğu bir **güvenlik göstergesi** kabul edilmektedir. Tüm ihtimalleri deneyerek bir şifreli verinin çözülmesini zamana yayarak imkansızlaştırmak için uzun anahtarlar kullanmak gerekir.

  Örneğin 8-bitlik bir anahtar 2^8=256 farklı çözme denemesi gerektirirken 56-bitlik bir anahtar için 2^{56}= $72x10^{15}$ deneme gerekmektedir.

Modern Dönem Kriptografi Algoritmalar

- 1947'de Bipolar transistor'ün icadıyla teknolojik ilerleme ivmelenmeye başlamıştır.
- 1958'de Jack Kilby (Texas Instruments), ilk hibrit tümleşik devreyi,
- 1959'da Robert Noyce, Mohammad Attala (Fairchild), ilk monolitik tümleşik devreyi geliştirmiştir.
- Bu gelişmeler sayesinde Kriptografi artık elektromekanik değil transistor ve lojik kapılarla elektronik olarak gerçekleştirilmeye başlar.

Modern Dönem Kriptografi Algoritmalar

20. yüzyılın ortasından itibaren yaşanan bu gelişmeler ile kriptografi alanında artık mekanik dönem kapanmış ve elektro-manyetik dönem başlamıştır.

Temel Kavramlar

Bipolar transistör, yarı iletken malzemelerden yapılan ve elektrik sinyallerini kontrol etmek için kullanılan bir elektronik bileşendir.

Temel Kavramlar

Hibrit tümleşik devreler, karmaşık bir entegre devre tasarımının bazı bileşenlerinin yonga üzerine entegre edilmesini gerektiren ancak diğer bileşenlerin daha büyük güç kapasitesi, yüksek sıcaklık toleransı veya daha yüksek güç yoğunluğu gereksinimleri gibi nedenlerle ayrı ayrı monte edilmesi gerektiği durumlarda kullanılır. Hibrit devrelerde, entegre devre teknolojisi genellikle mikroçipler gibi küçük, karmaşık fonksiyonları yerine getiren bileşenlerin üretimi için kullanılırken, diskret bileşenler (örneğin, transistörler, dirençler, kapasitörler) daha büyük güç ve performans gereksinimlerini karşılamak için kullanılır.

KAYNAKLAR

Procenne Digital Security

Emre GÖNCÜ

Abdullah VARICI