Kriptografi ve Siber Güvenlik

Cihangir TEZCAN

Department of Mathematics, METU

Institute of Informatics, CyDeS Cyber Defence and Security Laboratory, METU

Institute of Applied Mathematics, Department of Cryptography, METU

Middle East Technical University
February 12, 2015
Ankara, Turkey

Outline

Outline

Outline

Outline

Temel Amaçlar

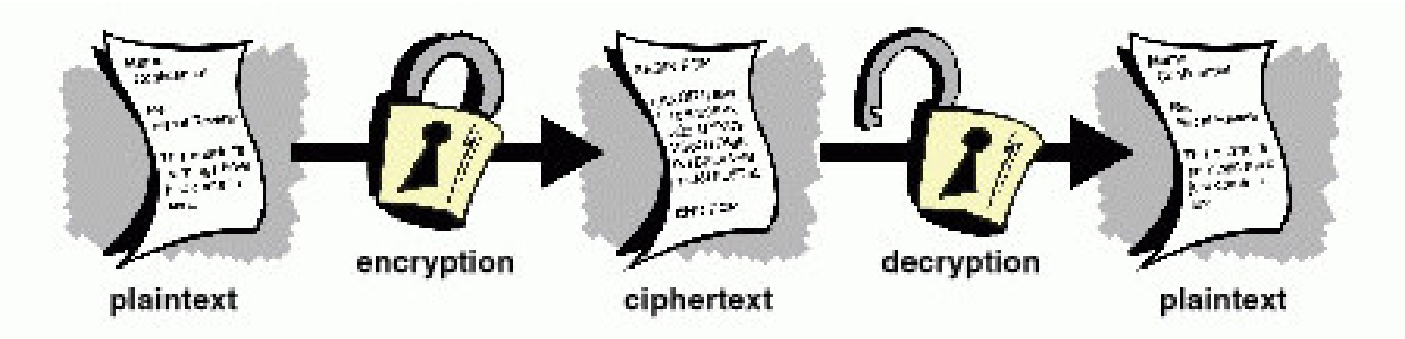
Temel Amaçlar

- **Gizlilik:** Bilgi istenmeyen kişiler tarafından anlaşılamamalıdır.
- **Bütünlük:** Bilginin iletilirken hiç değiştirilmemiş olduğu doğrulanmalıdır.
- **Kimlik Denetimi:** Gönderici ve alıcı birbirlerinin kimlikleri doğrulamalıdır.
- **İnkar Edememe:** Gönderici bilgiyi gönderdiğini inkar edememelidir.

Kriptosistem/Şifre ne demektir?

Kriptosistem/Şifre ne demektir?

- Korumak istediğiniz şey **düz metin**
- **Şifreli metin** düz metinin şifrelenmiş halidir
- Düz metinden şifreli metin oluşturan ve şifreli metni düz metne geri dönüştüren algoritmalara **kriptosistem/şifre** denir
- Şifreli metin *rastgele* (random) karakterler dizisi gibi gözükmelidir



Encoding

The ASCII code

American Standard Code for Information Interchange

www.theasciicode.com.ar

ASCII control characters

DEC	HEX	Simbolo ASCII	
00	00h	NULL	(carácter nulo)
01	01h	SOH	(inicio encabezado)
02	02h	STX	(inicio texto)
03	03h	ETX	(fin de texto)
04	04h	EOT	(fin transmisión)
05	05h	ENQ	(enquiry)
06	06h	ACK	(acknowledgement)
07	07h	BEL	(timbre)
08	08h	BS	(retroceso)
09	09h	HT	(tab horizontal)
10	0Ah	LF	(salto de linea)
11	0Bh	VT	(tab vertical)
12	0Ch	FF	(form feed)
13	0Dh	CR	(retorno de carro)
14	0Eh	SO	(shift Out)
15	0Fh	SI	(shift In)
16	10h	DLE	(data link escape)
17	11h	DC1	(device control 1)
18	12h	DC2	(device control 2)
19	13h	DC3	(device control 3)
20	14h	DC4	(device control 4)
21	15h	NAK	(negative acknowle.)
22	16h	SYN	(synchronous idle)
23	17h	ETB	(end of trans. block)
24	18h	CAN	(cancel)
25	19h	EM	(end of medium)
26	1Ah	SUB	(substitute)
27	1Bh	ESC	(escape)
28	1Ch	FS	(file separator)
29	1Dh	GS	(group separator)
30	1Eh	RS	(record separator)
31	1Fh	US	(unit separator)
127	20h	DEL	(delete)

ASCII printable characters

DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo
32	20h	espacio	64	40h	@	96	60h	`
33	21h	!	65	41h	A	97	61h	a
34	22h	"	66	42h	B	98	62h	b
35	23h	#	67	43h	C	99	63h	c
36	24h	$	68	44h	D	100	64h	d
37	25h	%	69	45h	E	101	65h	e
38	26h	&	70	46h	F	102	66h	f
39	27h	'	71	47h	G	103	67h	g
40	28h	(	72	48h	H	104	68h	h
41	29h	)	73	49h	I	105	69h	i
42	2Ah	*	74	4Ah	J	106	6Ah	j
43	2Bh	+	75	4Bh	K	107	6Bh	k
44	2Ch	,	76	4Ch	L	108	6Ch	l
45	2Dh	-	77	4Dh	M	109	6Dh	m
46	2Eh	.	78	4Eh	N	110	6Eh	n
47	2Fh	/	79	4Fh	O	111	6Fh	o
48	30h	0	80	50h	P	112	70h	p
49	31h	1	81	51h	Q	113	71h	q
50	32h	2	82	52h	R	114	72h	r
51	33h	3	83	53h	S	115	73h	s
52	34h	4	84	54h	T	116	74h	t
53	35h	5	85	55h	U	117	75h	u
54	36h	6	86	56h	V	118	76h	v
55	37h	7	87	57h	W	119	77h	w
56	38h	8	88	58h	X	120	78h	x
57	39h	9	89	59h	Y	121	79h	y
58	3Ah	:	90	5Ah	Z	122	7Ah	z
59	3Bh	;	91	5Bh	[	123	7Bh	{
60	3Ch	<	92	5Ch	\	124	7Ch	|
61	3Dh	=	93	5Dh	]	125	7Dh	}
62	3Eh	>	94	5Eh	^	126	7Eh	~
63	3Fh	?	95	5Fh	_			

theASCIIcode.com.ar

Extended ASCII characters

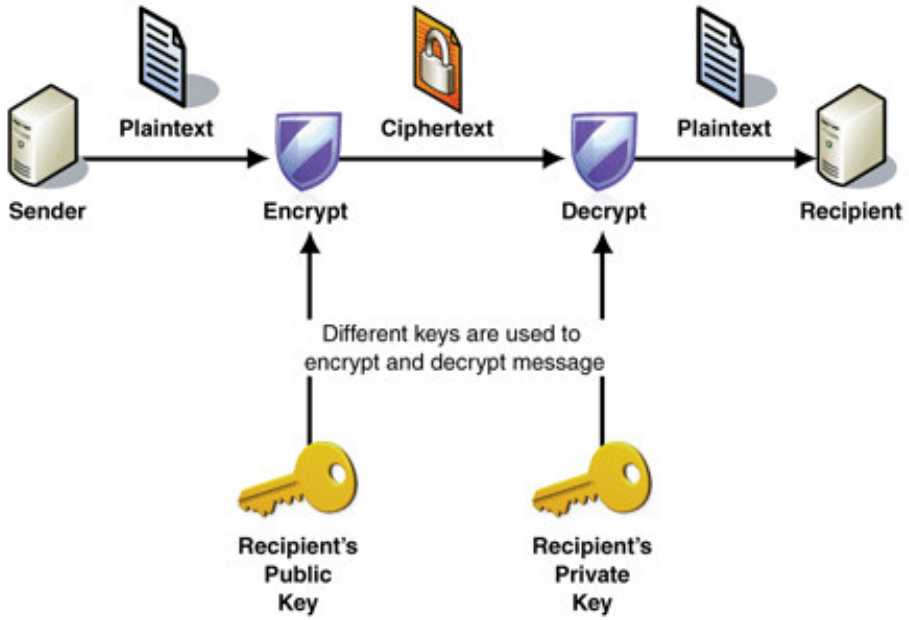
DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo
128	80h	Ç	160	A0h	á	192	C0h	└	224	E0h	Ó
129	81h	ü	161	A1h	í	193	C1h	┴	225	E1h	ß
130	82h	é	162	A2h	ó	194	C2h	┬	226	E2h	Ô
131	83h	â	163	A3h	ú	195	C3h	├	227	E3h	Ò
132	84h	ä	164	A4h	ñ	196	C4h	─	228	E4h	õ
133	85h	à	165	A5h	Ñ	197	C5h	┼	229	E5h	Õ
134	86h	å	166	A6h	ª	198	C6h	ã	230	E6h	µ
135	87h	ç	167	A7h	º	199	C7h	Ã	231	E7h	þ
136	88h	ê	168	A8h	¿	200	C8h	╚	232	E8h	Þ
137	89h	ë	169	A9h	®	201	C9h	╔	233	E9h	Ú
138	8Ah	è	170	AAh	¬	202	CAh	╩	234	EAh	Û
139	8Bh	ï	171	ABh	½	203	CBh	╦	235	EBh	Ù
140	8Ch	î	172	ACh	¼	204	CCh	╠	236	ECh	ý
141	8Dh	ì	173	ADh	¡	205	CDh	═	237	EDh	Ý
142	8Eh	Ä	174	AEh	«	206	CEh	╬	238	EEh	¯
143	8Fh	Å	175	AFh	»	207	CFh	¤	239	EFh	´
144	90h	É	176	B0h	░	208	D0h	ð	240	F0h	≡
145	91h	æ	177	B1h	▒	209	D1h	Ð	241	F1h	±
146	92h	Æ	178	B2h	▓	210	D2h	Ê	242	F2h	‗
147	93h	ô	179	B3h	│	211	D3h	Ë	243	F3h	¾
148	94h	ö	180	B4h	┤	212	D4h	È	244	F4h	¶
149	95h	ò	181	B5h	Á	213	D5h	ı	245	F5h	§
150	96h	û	182	B6h	Â	214	D6h	Í	246	F6h	÷
151	97h	ù	183	B7h	À	215	D7h	Î	247	F7h	¸
152	98h	ÿ	184	B8h	©	216	D8h	Ï	248	F8h	°
153	99h	Ö	185	B9h	╣	217	D9h	┘	249	F9h	¨
154	9Ah	Ü	186	BAh	║	218	DAh	┌	250	FAh	·
155	9Bh	ø	187	BBh	╗	219	DBh	█	251	FBh	¹
156	9Ch	£	188	BCh	╝	220	DCh	▄	252	FCh	³
157	9Dh	Ø	189	BDh	¢	221	DDh	¦	253	FDh	²
158	9Eh	×	190	BEh	¥	222	DEh	Ì	254	FEh	■
159	9Fh	ƒ	191	BFh	┐	223	DFh	▀	255	FFh	

Simetrik Kriptosistemler

- Şifreleme ve deşifreleme için kullanılan anahtarlar aynı ya da birbiriyle yakın ilişkilidir
- Yani, anahtarın biri, diğer anahtardan kolaylıkla elde edilebilmelidir (in polynomial time)

Asimetrik/Açık Anahtarlı Kriptosistemler

- Şifreleme anahtarı herkesin ulaşabileceği şekilde açıktadır
- Deşifreleme anahtarını elde etmek **zordur**



Kırılamayan Şifre

Kırılamayan Şifre (One-time pad)

- **Rastgele** bitlerden oluşan çok uzun bir dizi oluşturun (one-time pad)
- Şifreli metin elde etmek için, düz metni one-time pad ile XOR'layın
- Düz metni elde etmek için, şifreli metni one-time pad ile XOR'layın

Kırılamayan Şifre

Kırılamayan Şifre (One-time pad)

- **Rastgele** bitlerden oluşan çok uzun bir dizi oluşturun (one-time pad)
- Şifreli metin elde etmek için, düz metni one-time pad ile XOR'layın
- Düz metni elde etmek için, şifreli metni one-time pad ile XOR'layın

Example

Düz metin	010101111001001...
One-time pad	101111010110101...
Şifreli metin	111010101111100...

Kırılamayan Şifre

Kırılamayan Şifre (One-time pad)

- **Rastgele** bitlerden oluşan çok uzun bir dizi oluşturun (one-time pad)
- Şifreli metin elde etmek için, düz metni one-time pad ile XOR'layın
- Düz metni elde etmek için, şifreli metni one-time pad ile XOR'layın

Example

Düz metin	010101111001001...
One-time pad	101111010110101...
Şifreli metin	111010101111100...

Dikkat

- One-time pad **gerçekten rastgele** olmalıdır
- Her one-time pad **sadece bir kez** kullanılabilir

Akan Şifreler

Simetrik Şifreler iki sınıfa ayrılır

1. Akan Şifreler
2. Blok Şifreler

Akan Şifreler

Simetrik Şifreler iki sınıfa ayrılır

1. Akan Şifreler
2. Blok Şifreler

Akan Şifreler

- One-time pad kullanmak yerine, daha kısa bir anahtar kullanılır (örneğin 128 bits)
- Bu anahtar kullanılarak, uzun bir *sözde* rastgele *anahtar dizisi* oluşturulur ve bu dizi one-time pad gibi kullanılır
- Şifrenin güvenliği çoğunlukla anahtar dizisinin rastgeleliğine bağlıdır

Akan Şifreler

Simetrik Şifreler iki sınıfa ayrılır

1. Akan Şifreler
2. Blok Şifreler

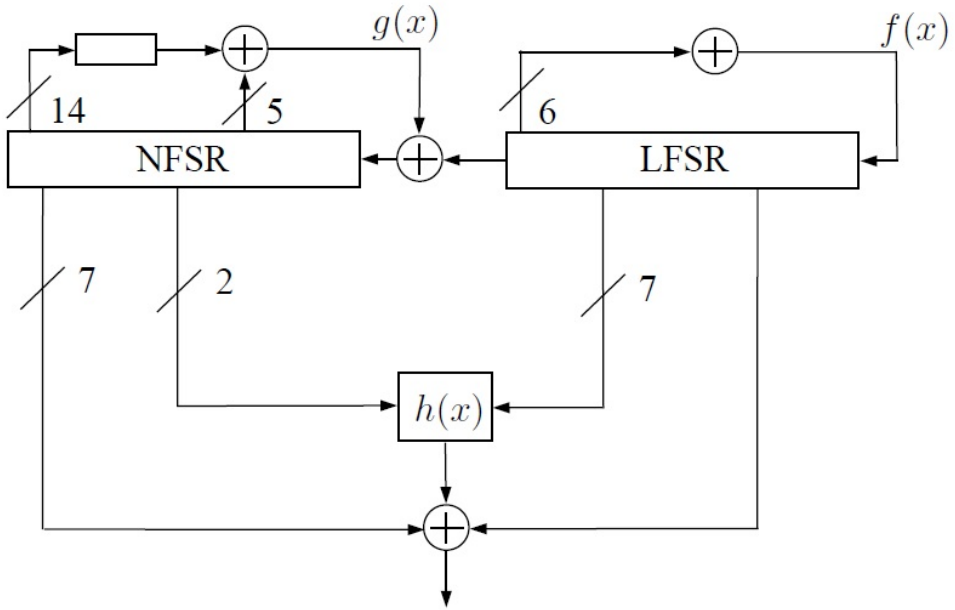
Akan Şifreler

- One-time pad kullanmak yerine, daha kısa bir anahtar kullanılır (örneğin 128 bits)
- Bu anahtar kullanılarak, uzun bir *sözde* rastgele *anahtar dizisi* oluşturulur ve bu dizi one-time pad gibi kullanılır
- Şifrenin güvenliği çoğunlukla anahtar dizisinin rastgeleliğine bağlıdır

Dikkat

Anahtar dizisi artık *gerçekten rastgele* değil, *sözde rastgele*dir

Akan Şifre Örneği: Grain



- $f(x) = 1 + x^{32} + x^{47} + x^{58} + x^{90} + x^{121} + x^{128}$
- $g(x) = 1 + x^{32} + x^{37} + x^{72} + x^{102} + x^{128} + x^{44}x^{60} + x^{61}x^{125} + x^{63}x^{67} + x^{69}x^{101} + x^{80}x^{88} + x^{110}x^{11} + x^{115}x^{117}$
- $h(x) = x_0x_1 + x_2x_3 + x_4x_5 + x_6x_7 + x_0x_4x_8$

Akan Şifreler

Genellikle blok şifrelerden çok daha hızlıdırlar

Bazı akan şifreler

- A5/1 (GSM)
- RC4 (WEP)
- E0 (Bluetooth)

Akan Şifreler

Genellikle blok şifrelerden çok daha hızlıdırlar

Bazı akan şifreler

- A5/1 (GSM)
- RC4 (WEP)
- E0 (Bluetooth)

Akan Şifreler

- 2004 yılında yapılan eStream yarışmasına katılan 34 aday algoritmadan 7 tanesi Eylül 2008'de kullanılabilir olarak seçildi ama standartlaştırmak için henüz erken olduğu belirtildi
- Donanım: Grain v1, MICKEY 2.0, Trivium
- Yazılım: HC-128, Rabbit, Salsa20/12, SOSEMANUK
- Trivium ISO/IEC standardı oldu (29192-3:2012)

Blok Şifreler

Blok Şifreler

Düz metin eşit uzunluklardaki (b bit) bloklara ayrılıp şifreleme işlemi bloklar üzerinden yapılır

Örnek Blok Şifre: PRESENT (ISO Standardı)

- Blok uzunluğu: 64 bit
- Anahtar uzunluğu: 80 ya da 128 bit
- Döngü sayısı: 31

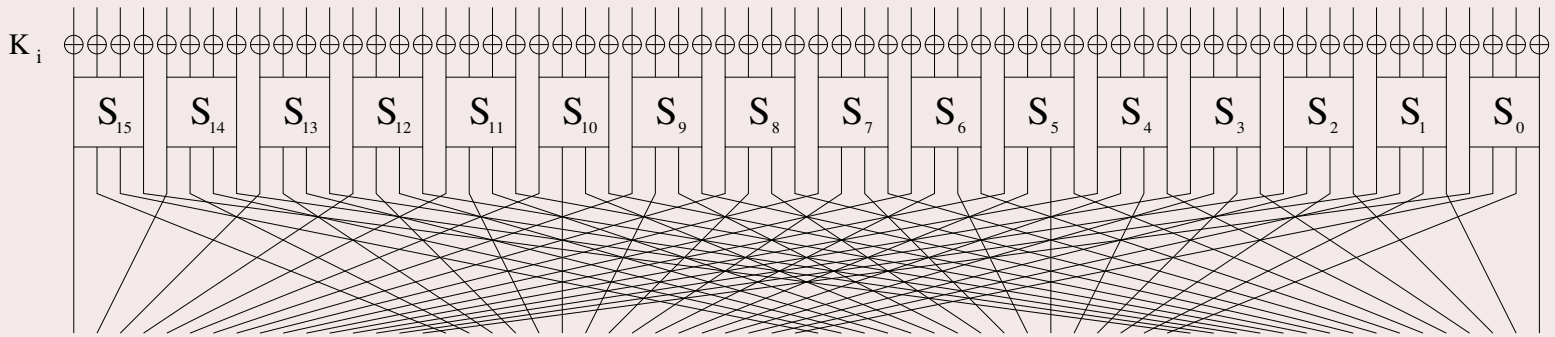
Blok Şifreler

Blok Şifreler

Düz metin eşit uzunluklardaki (b bit) bloklara ayrılıp şifreleme işlemi bloklar üzerinden yapılır

Örnek Blok Şifre: PRESENT (ISO Standardı)

- Blok uzunluğu: 64 bit
- Anahtar uzunluğu: 80 ya da 128 bit
- Döngü sayısı: 31



x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Standartlaştırılmış Blok Şifre

Data Encryption Standard (DES)

- 1970'te IBM dizayn etti (NSA değişiklik yaptı)
  - Blok uzunluğu: 64 bit
  - Anahtar uzunluğu : 56 bit
  - Döngü sayısı: 16
- Anahtarın kısa olması nedeniyle 1990lardan sonra kullanılamaz hale geldi

Standartlaştırılmış Blok Şifre

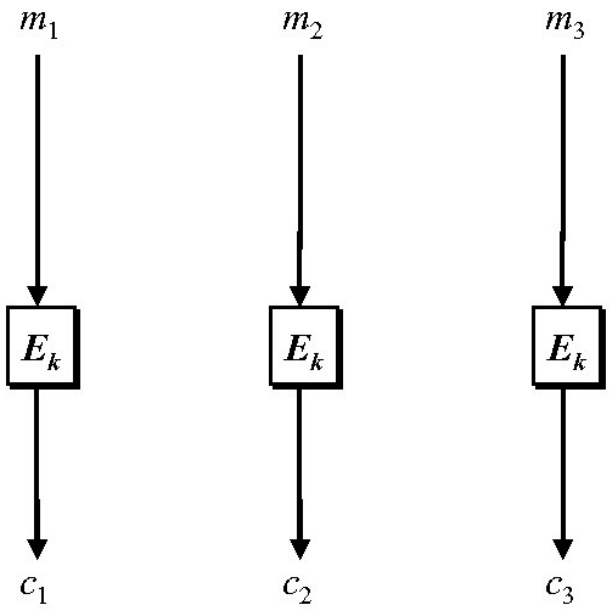
Data Encryption Standard (DES)

- 1970'te IBM dizayn etti (NSA değişiklik yaptı)
  - Blok uzunluğu: 64 bit
  - Anahtar uzunluğu : 56 bit
  - Döngü sayısı: 16
- Anahtarın kısa olması nedeniyle 1990lardan sonra kullanılamaz hale geldi

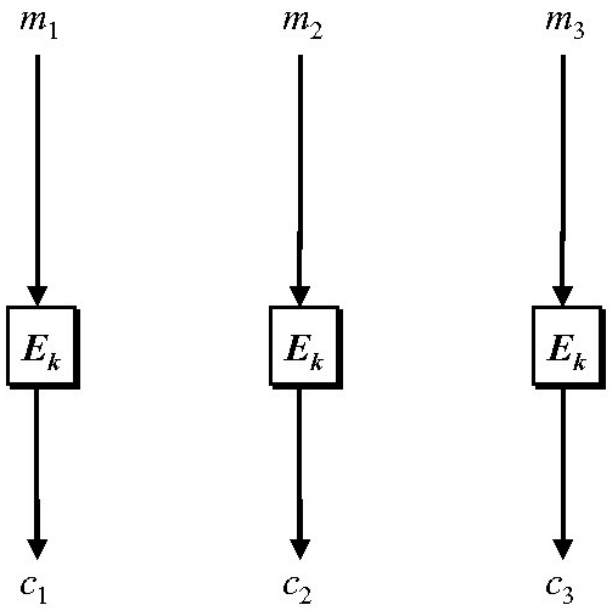
Advanced Encryption Standard (AES)

- 2001 yılında NIST standartlaştırdı (herkese açık olan yarışma birincisi)
  - Blok uzunluğu: 128 bit
  - Anahtar uzunluğu: 128, 192, 256 bit
  - Döngü sayısı: 10, 12, 14 (anahtar uzunluğuna göre)
- Bilinen bütün ataklar *etkisiz*

Blok Şifreler



Blok Şifreler



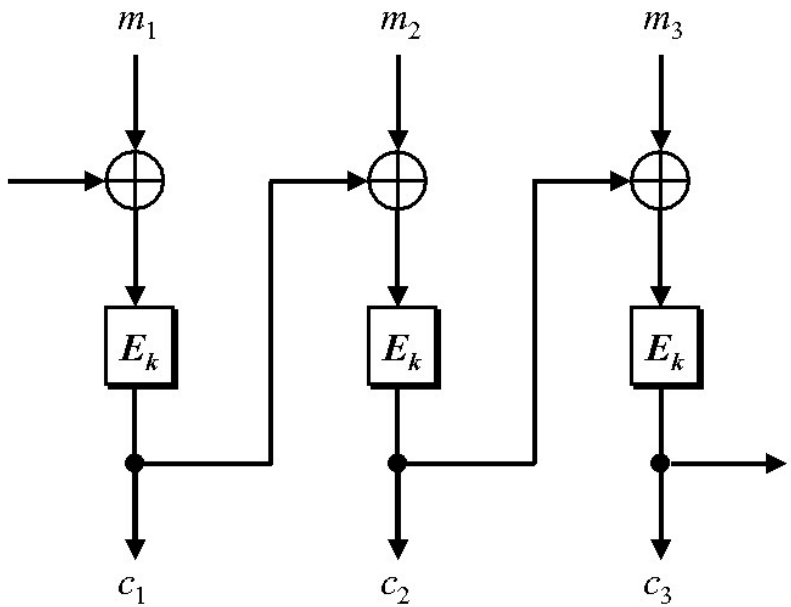
Problem

Her bloğun birbirinden bağımsız olarak şifrelernmesi tavsiye edilmez çünkü aynı düz metin blokları aynı şifreli metin bloklarına gidecektir.

Blok Şifreler

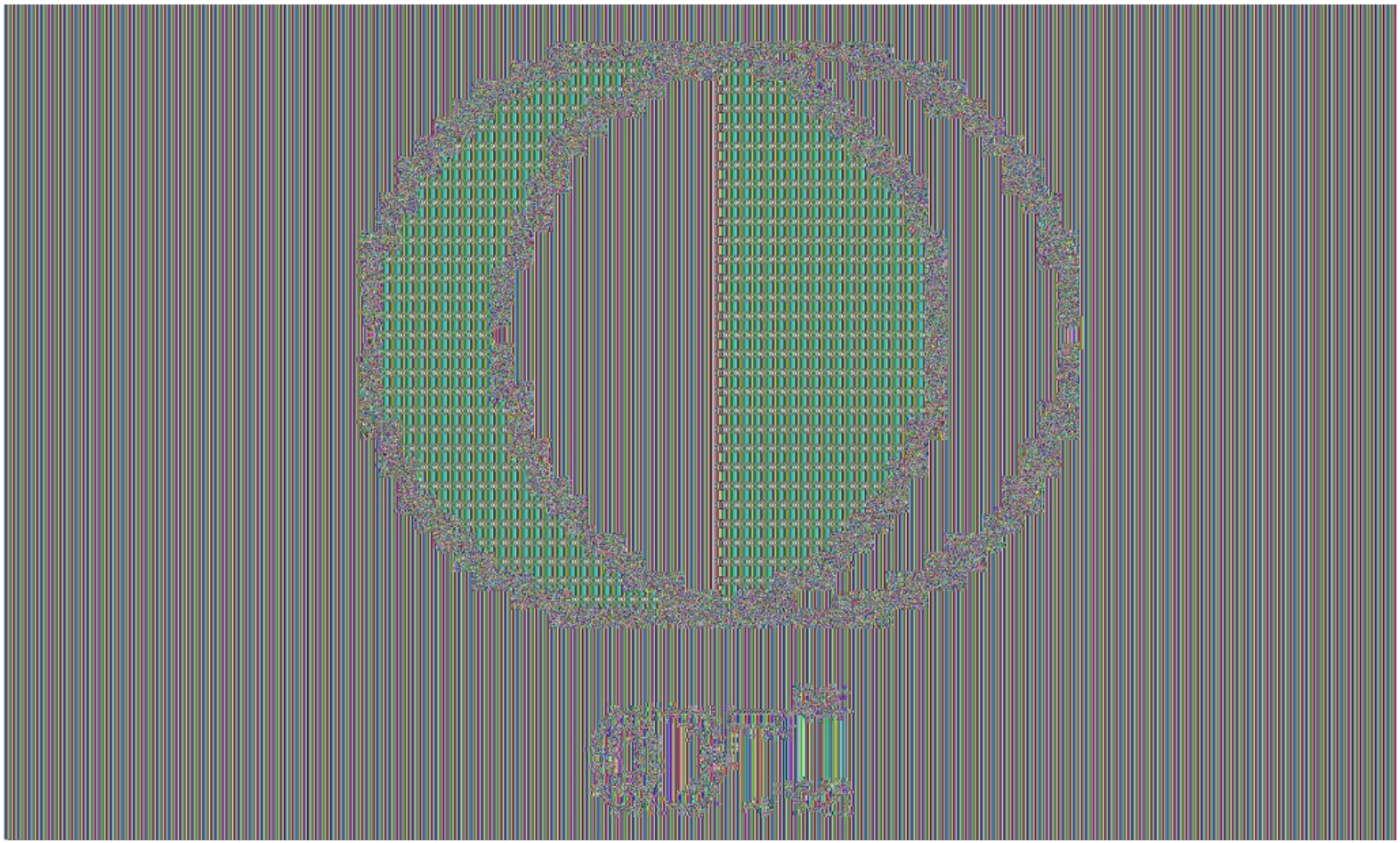
Çözüm

Bir çalışma türü (mode of operation) seçin. Örn: blok şifre zincirleme türü (Block cipher chaining mode)

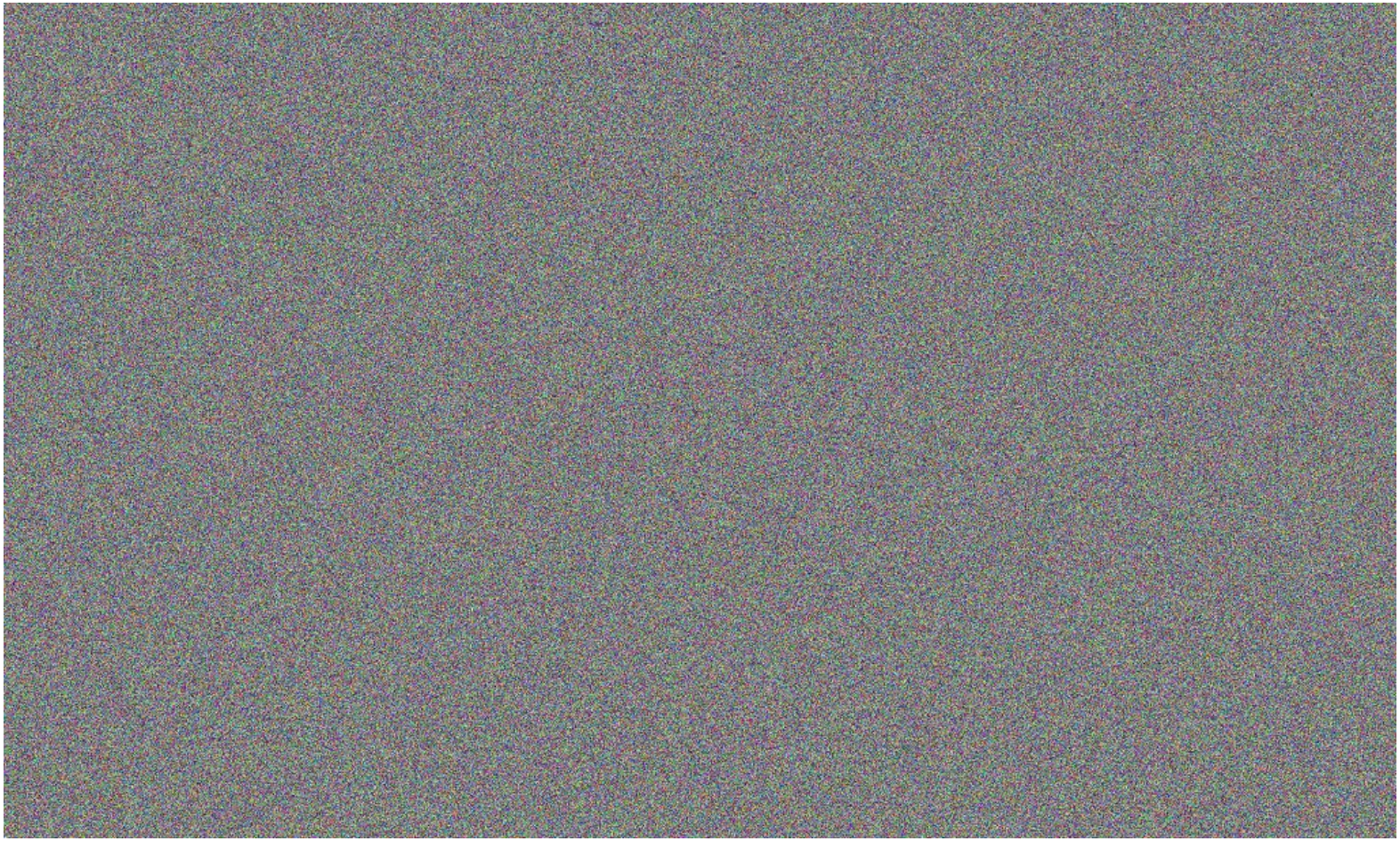


Blok Şifre Çalışma Şekilleri: Orjinal Resim

Blok Şifre Çalışma Şekilleri: AES-128 ECB

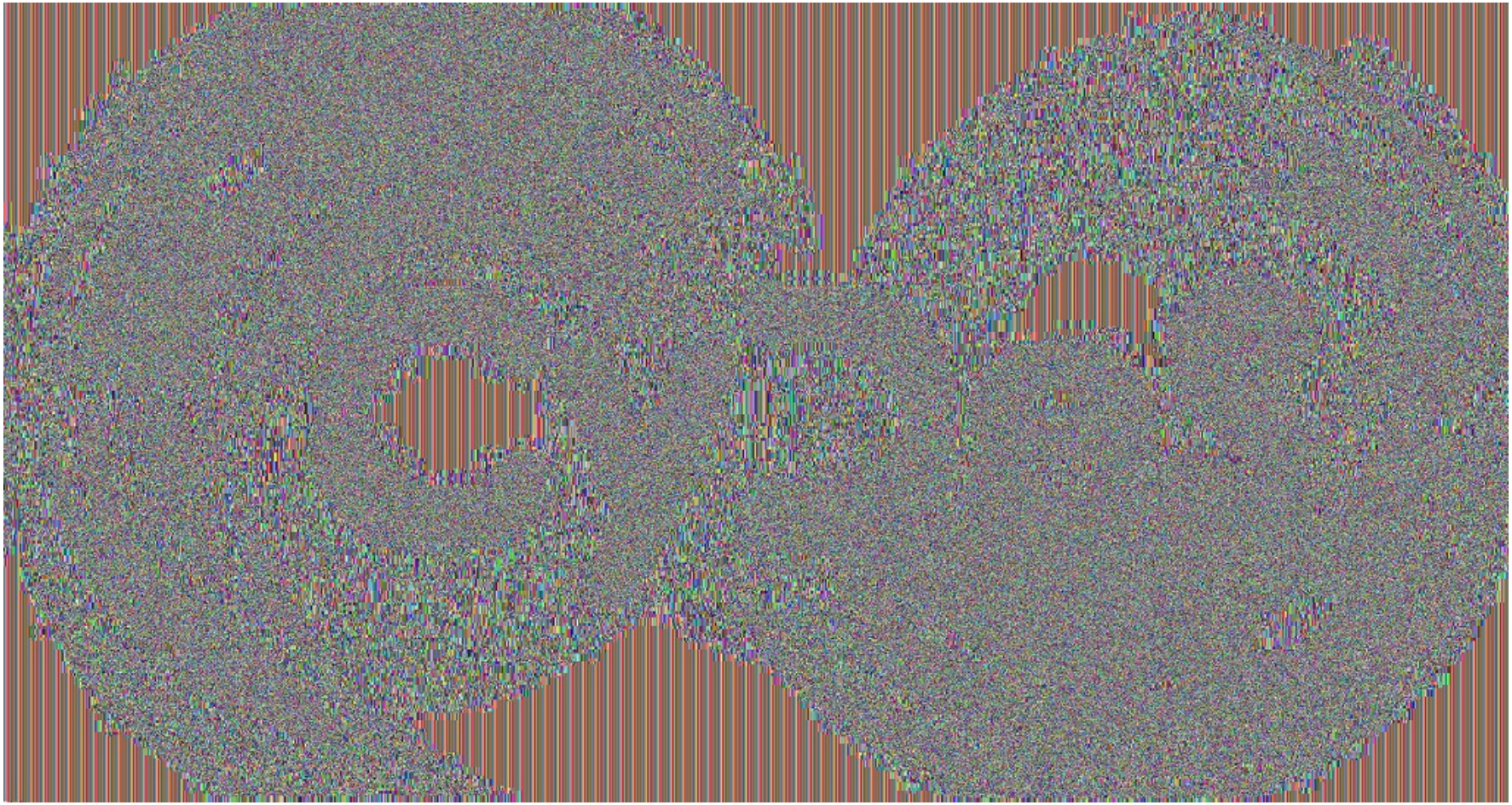


Blok Şifre Çalışma Şekilleri: AES-128 CTR

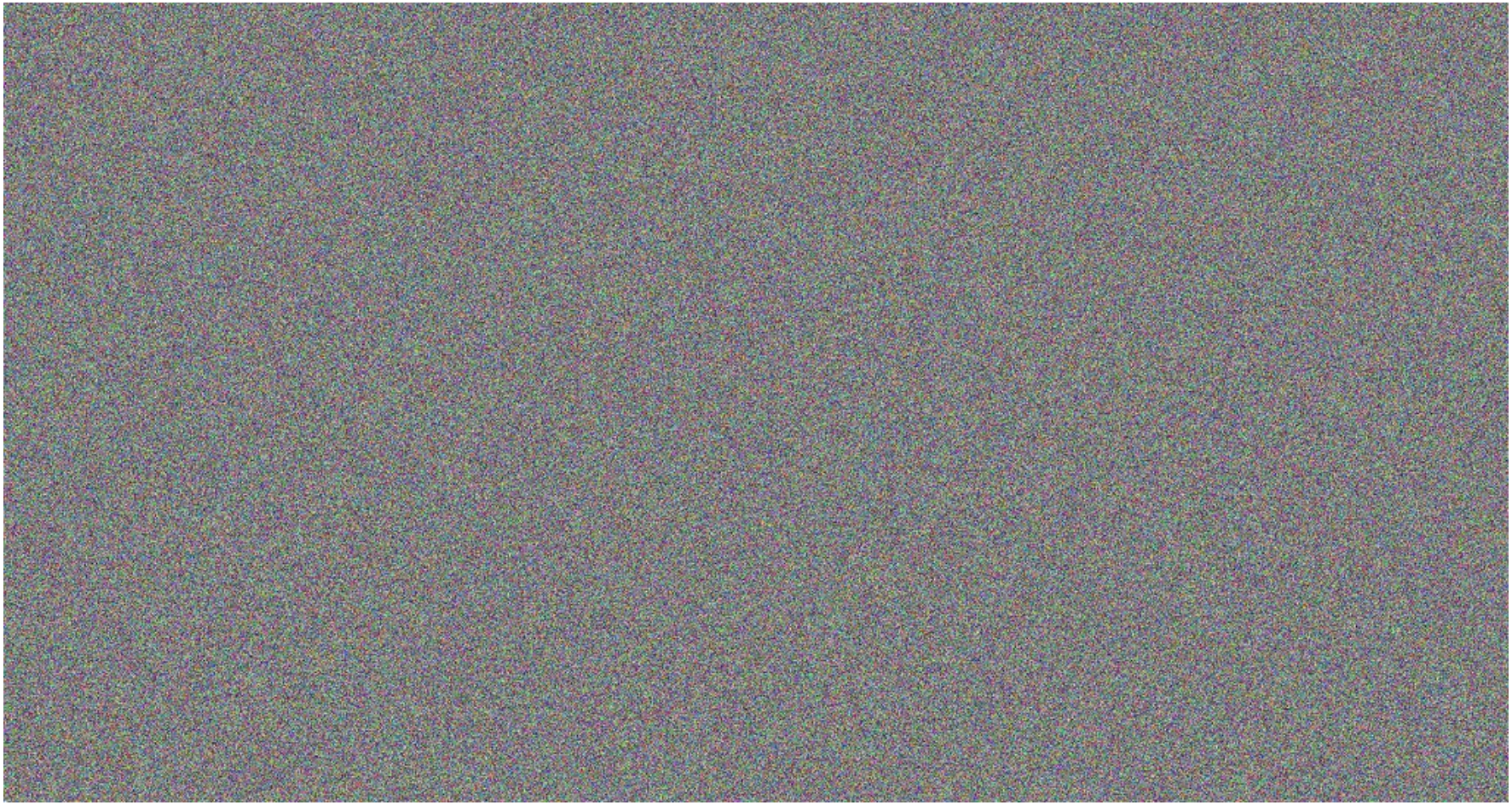


Blok Şifre Çalışma Şekilleri: Orjinal Resim

Blok Şifre Çalışma Şekilleri: AES-128 ECB



Blok Şifre Çalışma Şekilleri: AES-128 CTR



Asimetrik/Açık Anahtarlı Kriptografi

Asimetrik Kriptografi

- 1976 yılında Diffie ve Hellman tarafından önerilmiştir
- Daha önceden hiç görüşmemiş kişilerin güvenli haberleşmesini sağlar
- Kimlik doğrulama ve inkar edememe problemlerine çözüm sunar
- Güvenlik zor matematiksel problemlere dayanır
  - Çarpanlara ayırma problemi: RSA,...
  - Discrete logaritma problemi: El-gamal,...

Asimetrik/Açık Anahtarlı Kriptografi

Asimetrik Kriptografi

- 1976 yılında Diffie ve Hellman tarafından önerilmiştir
- Daha önceden hiç görüşmemiş kişilerin güvenli haberleşmesini sağlar
- Kimlik doğrulama ve inkar edememe problemlerine çözüm sunar
- Güvenlik zor matematiksel problemlere dayanır
  - Çarpanlara ayırma problemi: RSA,...
  - Discrete logaritma problemi: El-gamal,...
- Bilinen tüm asimetrik kriptosistemler işlemci zamanı ve bandwidth açısından masraflıdır

RSA

RSA (Rivest-Shamir-Adleman)

- Çok büyük (en az 512-bitlik) iki p ve q asal sayısı üretilir, $n = pq$ diyelim

RSA

RSA (Rivest-Shamir-Adleman)

- Çok büyük (en az 512-bitlik) iki p ve q asal sayısı üretilir, $n = pq$ diyelim
- $ed \equiv 1 \pmod{(p-1)(q-1)}$ denkliğini sağlayan e ve d sayıları seçilir ($e = 65537$ şifreleme işlemlerini kolaylaştırdığı için tavsiye edilir)

RSA

RSA (Rivest-Shamir-Adleman)

- Çok büyük (en az 512-bitlik) iki p ve q asal sayısı üretilir, $n = pq$ diyelim
- $ed \equiv 1 \pmod{(p-1)(q-1)}$ denkliğini sağlayan e ve d sayıları seçilir ($e = 65537$ şifreleme işlemlerini kolaylaştırdığı için tavsiye edilir)
- Açık anahtar: $< e, n >$, gizli anahtar: $< d, n >$

RSA

RSA (Rivest-Shamir-Adleman)

- Çok büyük (en az 512-bitlik) iki p ve q asal sayısı üretilir, $n = pq$ diyelim
- $ed \equiv 1 \pmod{(p-1)(q-1)}$ denkliğini sağlayan e ve d sayıları seçilir ($e = 65537$ şifreleme işlemlerini kolaylaştırdığı için tavsiye edilir)
- Açık anahtar: $< e, n >$, gizli anahtar: $< d, n >$
- Mesaj m'i şifrelemek için $c = m^e \pmod{n}$, deşifrelemek için $m = c^d \pmod{n}$ işlemleri uygulanır

RSA

RSA (Rivest-Shamir-Adleman)

- Çok büyük (en az 512-bitlik) iki p ve q asal sayısı üretilir, $n = pq$ diyelim
- $ed \equiv 1 \pmod{(p-1)(q-1)}$ denkliğini sağlayan e ve d sayıları seçilir ($e = 65537$ şifreleme işlemlerini kolaylaştırdığı için tavsiye edilir)
- Açık anahtar: $< e, n >$, gizli anahtar: $< d, n >$
- Mesaj m'i şifrelemek için $c = m^e \pmod{n}$, deşifrelemek için $m = c^d \pmod{n}$ işlemleri uygulanır
- Sistemin güvenliği *çoğunlukla* n sayısının çarpanlarına ayrılmasına dayanır

RSA

RSA (Rivest-Shamir-Adleman)

- Çok büyük (en az 512-bitlik) iki p ve q asal sayısı üretilir, $n = pq$ diyelim
- $ed \equiv 1 \pmod{(p-1)(q-1)}$ denkliğini sağlayan e ve d sayıları seçilir ($e = 65537$ şifreleme işlemlerini kolaylaştırdığı için tavsiye edilir)
- Açık anahtar: $< e, n >$, gizli anahtar: $< d, n >$
- Mesaj m'i şifrelemek için $c = m^e \pmod{n}$, deşifrelemek için $m = c^d \pmod{n}$ işlemleri uygulanır
- Sistemin güvenliği *çoğunlukla* n sayısının çarpanlarına ayrılmasına dayanır
- Bu tarz büyük asal sayılar bulmak kolaydır ama n'i çarpanlarına ayırmanın zor olduğuna **inanılır**

Kriptanaliz

Exhaustive Search (kaba kuvvet)

- Mümkün olan her anahtarı tek tek deneyin
- k bit anahtar için 2^k şifreleme işlemi gereklidir (Güvenlik üst sınırı)

Kriptanaliz

Exhaustive Search (kaba kuvvet)

- Mümkün olan her anahtarı tek tek deneyin
- k bit anahtar için 2^k şifreleme işlemi gereklidir (Güvenlik üst sınırı)

Kaba kuvvet atakları ne kadar zor

$\mathbf{2^{80} = 1.208.925.819.614.629.174.706.176}$

Kriptanaliz

Exhaustive Search (kaba kuvvet)

- Mümkün olan her anahtarı tek tek deneyin
- k bit anahtar için 2^k şifreleme işlemi gereklidir (Güvenlik üst sınırı)

Kaba kuvvet atakları ne kadar zor

$\mathbf{2^{80} = 1.208.925.819.614.629.174.706.176}$
$\mathbf{2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456}$

Kriptanaliz

Exhaustive Search (kaba kuvvet)

- Mümkün olan her anahtarı tek tek deneyin
- k bit anahtar için 2^k şifreleme işlemi gereklidir (Güvenlik üst sınırı)

Kaba kuvvet atakları ne kadar zor

2^{80}= 1.208.925.819.614.629.174.706.176
2^{128}= 340.282.366.920.938.463.463.374.607.431.768.211.456
2^{192}= 6.277.101.735.386.680.763.835.789.423.207.666.416
102.355.444.464.034.512.896

Kriptanaliz

Exhaustive Search (kaba kuvvet)

- Mümkün olan her anahtarı tek tek deneyin
- k bit anahtar için 2^k şifreleme işlemi gereklidir (Güvenlik üst sınırı)

Kaba kuvvet atakları ne kadar zor

$2^{80} = 1.208.925.819.614.629.174.706.176$
$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$
$2^{192} = 6.277.101.735.386.680.763.835.789.423.207.666.416$
$102.355.444.464.034.512.896$
$2^{256} = 115.792.089.237.316.195.423.570.985.008.687.907.853$
$269.984.665.640.564.039.457.584.007.913.129.639.936$

Kriptanaliz

Kaba kuvvet atağı: PRESENT-80

İşlemci	Çekirdek Sayısı	Hız	Şifreleme İşlemi Sayısı	Atak Süresi
i7-2630QM	4	2.0GHz	15.430.000/s	2.484.432.032 yıl
i7-4770	4	3.4GHz	31.410.000/s	1.220.464.382 yıl

Kriptanaliz

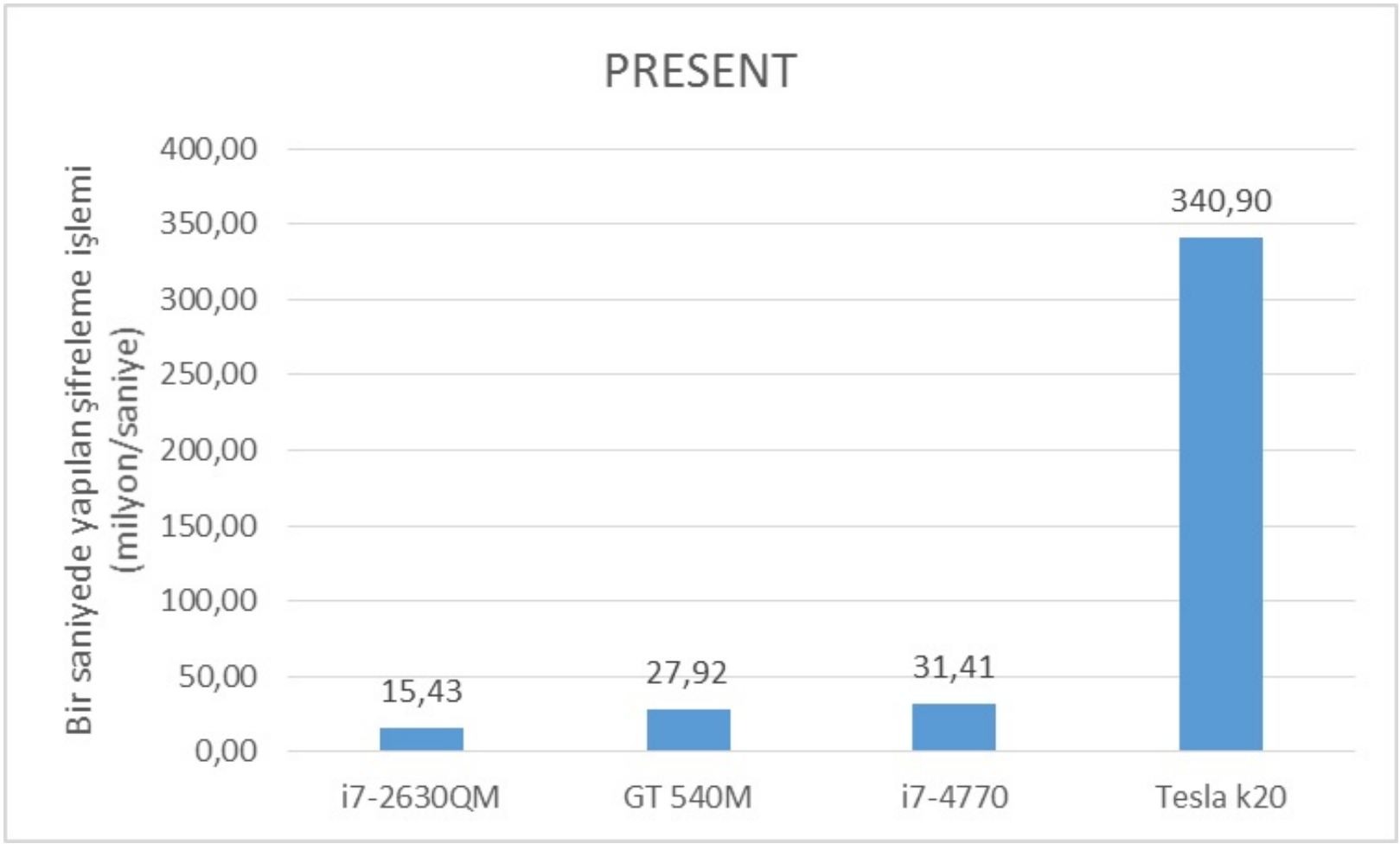
Kaba kuvvet atağı: PRESENT-80

İşlemci	Çekirdek Sayısı	Hız	Şifreleme İşlemi Sayısı	Atak Süresi
i7-2630QM	4	2.0GHz	15.430.000/s	2.484.432.032 yıl
i7-4770	4	3.4GHz	31.410.000/s	1.220.464.382 yıl

Kaba kuvvet atağı: PRESENT-80 (Ekran Kartları)

İşlemci	Çekirdek Sayısı	Hız	Şifreleme İşlemi Sayısı	Atak Süresi
GT 540M	96	1.34GHz	27.920.000/s	1.373.022.430 yıl
Tesla k20	2496	0.71GHz	340.900.000/s	112.451.705 yıl

PRESENT-80 Kriptanaliz Hız testi



Kriptanaliz

Kriptanaliz Yöntemleri

- Diferansiyel Kriptanaliz (Biham, Shamir 1980s)
  - Truncated Differential Cryptanalysis (Knudsen 1994)
  - Higher Order Differential Cryptanalysis (Knudsen 1994)
  - Impossible Differential Cryptanalysis (Biham-Biryukov-Shamir 1998)
  - Boomerang Attack (Wagner 1999)
  - Improbable Differential Cryptanalysis (Tezcan 2010)
- Lineer Kriptanaliz (Matsui 1992)
- Cebirsel Kriptanaliz (Courtois, Pieprzyk 2002)

Özet Fonksiyonlar

Özet Fonksiyonlar

- Girdi hangi uzunlukta olursa olsun, çıktı uzunluğu sabittir (128-bit, 192-bit,...)

Özet Fonksiyonlar

Özet Fonksiyonlar

- Girdi hangi uzunlukta olursa olsun, çıktı uzunluğu sabittir (128-bit, 192-bit,...)
- Aynı çıktıyı verecek iki farklı girdi bulmak zor olmalıdır (Collision resistance)

Özet Fonksiyonlar

Özet Fonksiyonlar

- Girdi hangi uzunlukta olursa olsun, çıktı uzunluğu sabittir (128-bit, 192-bit,...)
- Aynı çıktıyı verecek iki farklı girdi bulmak zor olmalıdır (Collision resistance)
- Sadece çıktıdan, girdiyi elde etmek zor olmalıdır (Pre-image resistance)

Özet Fonksiyonlar

Özet Fonksiyonlar

- Girdi hangi uzunlukta olursa olsun, çıktı uzunluğu sabittir (128-bit, 192-bit,...)
- Aynı çıktıyı verecek iki farklı girdi bulmak zor olmalıdır (Collision resistance)
- Sadece çıktıdan, girdiyi elde etmek zor olmalıdır (Pre-image resistance)
- Bir girdi ve karşılık gelen çıktı verildiğinde, aynı çıktıyı verecek ikinci bir girdi bulmak zor olmalıdır (Second pre-image resistance)

Özet Fonksiyonlar

Bazı Özet Fonksiyonlar

- MD4 (Ron Rivest, 1990lar) **kırıldı**
- MD5 (Ron Rivest, 1990lar) **kırıldı**
- SHA-0, SHA-1 (NSA, 1990lar, MD4/MD5 tabanlı) **kırıldı**
- SHA-2 (NSA)
- Keccak (Ekim 2012, NIST yarışması kazananı)

Özet Fonksiyonlar

Bazı Özet Fonksiyonlar

- MD4 (Ron Rivest, 1990lar) **kırıldı**
- MD5 (Ron Rivest, 1990lar) **kırıldı**
- SHA-0, SHA-1 (NSA, 1990lar, MD4/MD5 tabanlı) **kırıldı**
- SHA-2 (NSA)
- Keccak (Ekim 2012, NIST yarışması kazananı)
  - 64 başvuru, 51'i ilk aşamaya yükseldi, 3'ü Türk
  - Shamata (Orhun Kara), **pratik olarak kırıldı**
  - Sarmal (Onur Özen, Kerem Varıcı, Çelebi Kocair), **teorik zayıflık**
  - Hamsi (Özgül Küçük), ilk 14'e kaldı ama **çok yavaş**

Kerkckhoffs Prensibi

Kerkckhoffs Prensibi (1883)

Şifre gizli tutulmak zorunda olmamalıdır ve şifrenin düşman eline geçmesi hiçbir sıkıntı oluşturmamalıdır.

Yani, sistemin güvenliği tamamiyle *anahtarın* gizli tutulmasına bağlı olmalıdır.

Claude Shannon

The enemy knows the system.

3 B's of Cryptography

Bribe, Burglary, Blackmail

Password Cracking

Parolalar

- Parolalar hizmet veren birimin veritabanında özet fonksiyonu çıktısı olarak tutulmalıdır

Password Cracking

Parolalar

- Parolalar hizmet veren birimin veritabanında özet fonksiyonu çıktısı olarak tutulmalıdır
- Birkaç yanlış parola girilmesinden sonra sistemin bir süre bağlantıya izin vermemesinin sebebi kaba kuvvet saldırılarını engellemek içindir

Password Cracking

Parolalar

- Parolalar hizmet veren birimin veritabanında özet fonksiyonu çıktısı olarak tutulmalıdır
- Birkaç yanlış parola girilmesinden sonra sistemin bir süre bağlantıya izin vermemesinin sebebi kaba kuvvet saldırılarını engellemek içindir
- İnternette 8 haneli şifrelerin güvenli olduğu algısı vardır ama bu varsayım CPU'lar düşünülerek elde edilmiştir

Password Cracking

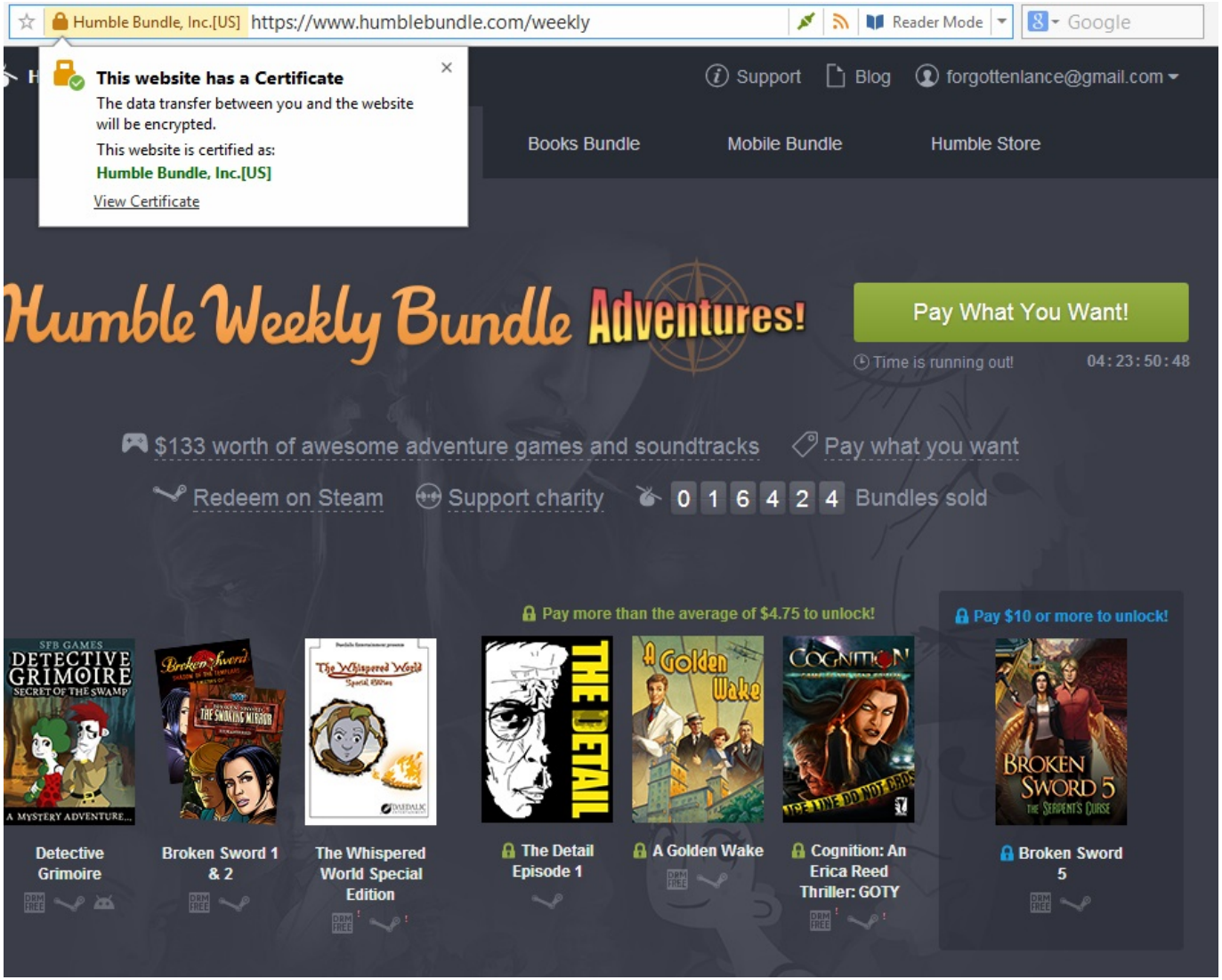
Parolalar

- Parolalar hizmet veren birimin veritabanında özet fonksiyonu çıktısı olarak tutulmalıdır
- Birkaç yanlış parola girilmesinden sonra sistemin bir süre bağlantıya izin vermemesinin sebebi kaba kuvvet saldırılarını engellemek içindir
- İnternette 8 haneli şifrelerin güvenli olduğu algısı vardır ama bu varsayım CPU'lar düşünülerek elde edilmiştir

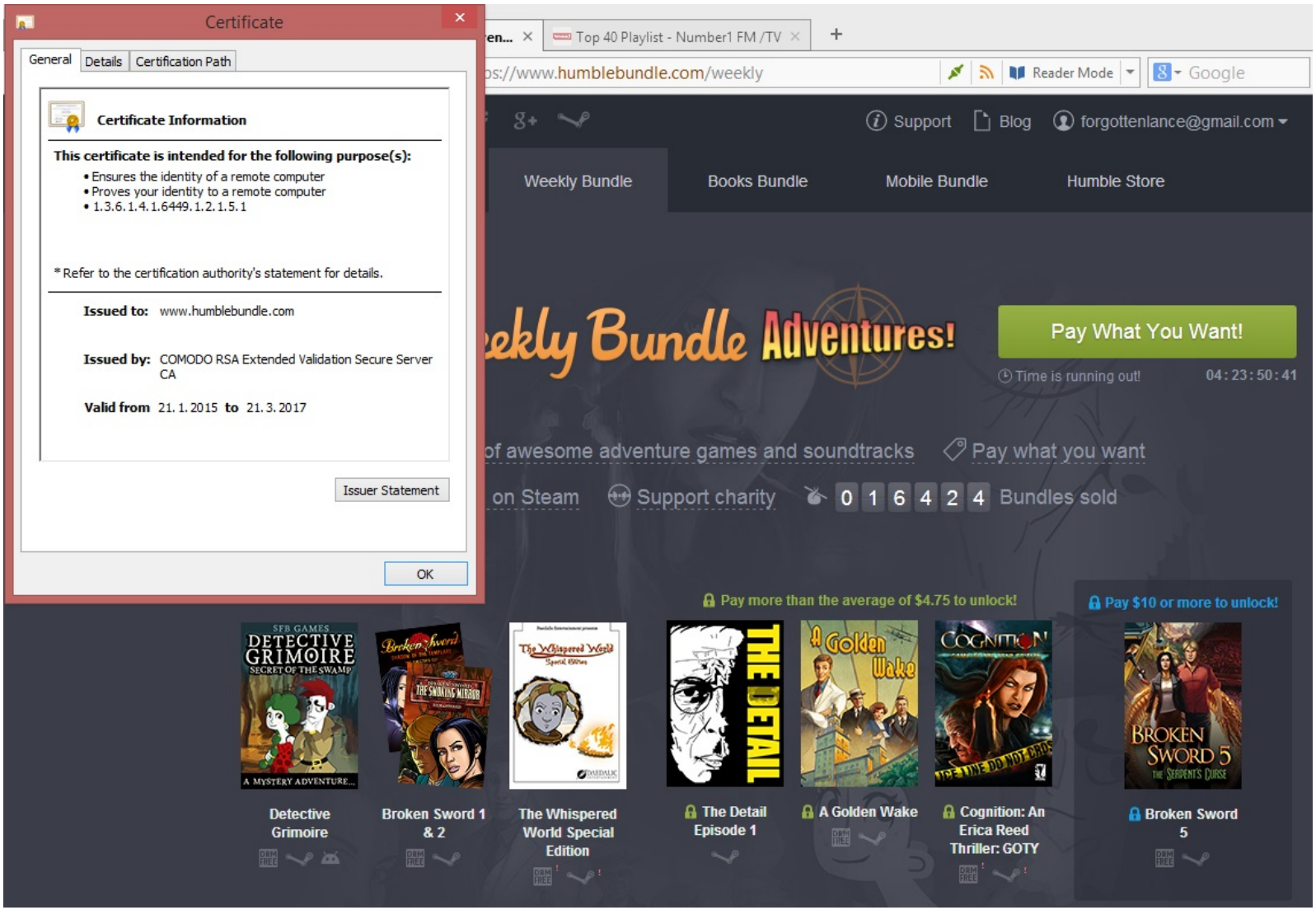
10 harfli şifrelere tek GPU kullanarak kaba kuvvet saldırısı yapmak

Küçük harfler (26 karakter)	18 saat
Harfler ve sayılar (62 karakter)	3.107 gün
Ekrana yazdırılabilir karakterler (94 karakter)	198.841 gün

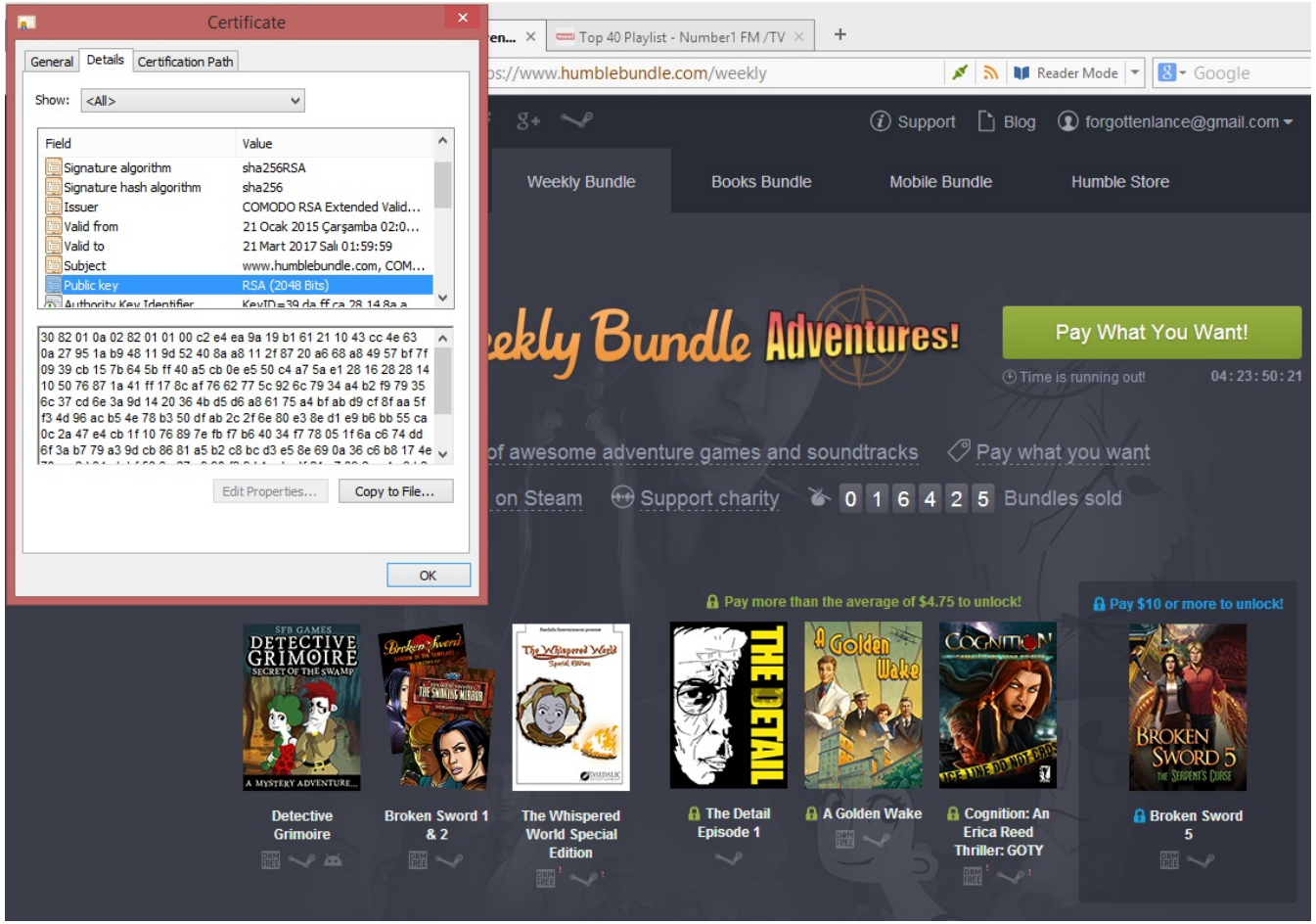
Kimlik Denetimi ve Bütünlük



Kimlik Denetimi ve Bütünlük



Kimlik Denetimi ve Bütünlük

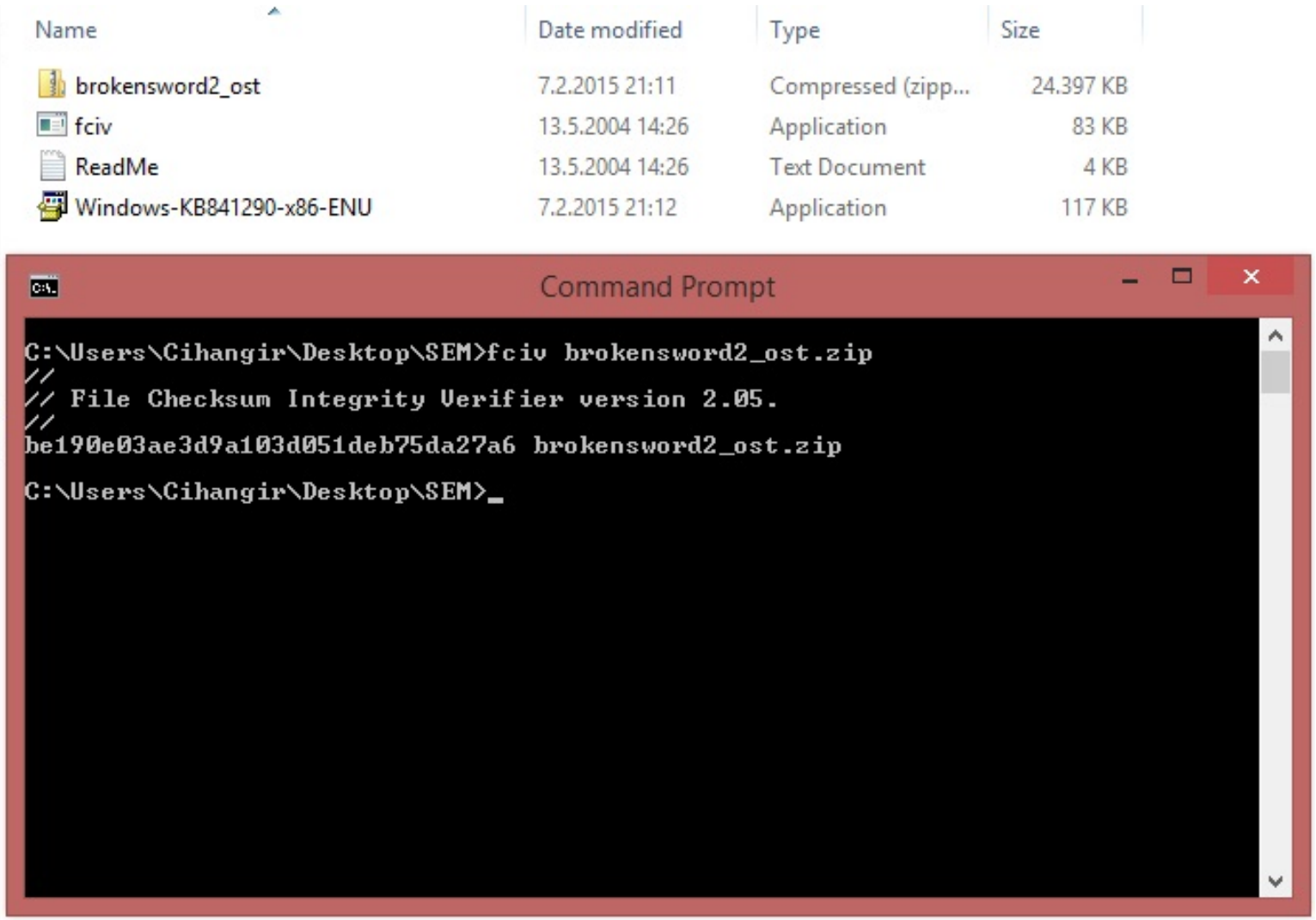


Broken Sword 2: The Smoking Mirror Soundtrack
Revolution Software

FLAC
85.9 MB md5

MP3
be190e03ae3
d9a103d051d
eb75da27a6

Kimlik Denetimi ve Bütünlük



Buluttaki dosyalarımız güvenli ellerde mi? (The Fappening)

iCloud

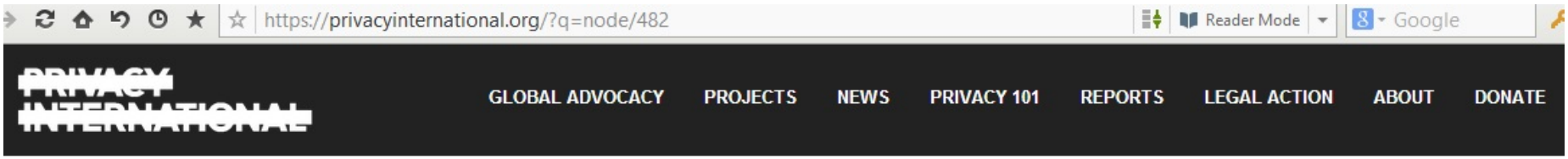
- 144+ ünlünün iPhone ile çektikleri kişisel fotoğraf ve videoları internete yüklendi
- Apple olayın iCloud'la ilgisi olduğunu yalanladı

Buluttaki dosyalarımız güvenli ellerde mi? (The Fappening)

iCloud

- 144+ ünlünün iPhone ile çektikleri kişisel fotoğraf ve videoları internete yüklendi
- Apple olayın iCloud'la ilgisi olduğunu yalanladı
- Nasıl yapıldı:
  - Adım 1: Ünlü birinin email adresini öğren
  - Adım 2: Find My iPhone hizmetindeki açığı kullanarak kaba kuvvet saldırısı yap
  - Adım 3: Resim, video, adres defteri, silinmiş dosyaları indir
  - Adım 4: Adres defterinden başka bir ünlünün email adresini öğren, Adım 1'e geri dön

Mass Surveillance



GCHQ-NSA INTELLIGENCE SHARING UNLAWFUL, SAYS UK SURVEILLANCE TRIBUNAL

Date:

Friday, February 6, 2015

British intelligence services acted unlawfully in accessing millions of people's personal communications collected by the NSA, the Investigatory Powers Tribunal ruled today. The decision marks the first time that the Tribunal, the only UK court empowered to oversee GHCQ, MI5 and MI6, has ever ruled against the intelligence and security services in its 15 year history.

The Tribunal declared that intelligence sharing between the United States and the United Kingdom was unlawful prior to December 2014, because the rules governing the UK's access to the NSA's PRISM and UPSTREAM programmes were secret. It was only due to revelations made during the course of this case, which relied almost entirely on documents disclosed by NSA whistleblower Edward Snowden, that the intelligence sharing relationship became subject to public scrutiny.

The claimants in the case are Privacy International, Bytes for All, Liberty, and Amnesty International.

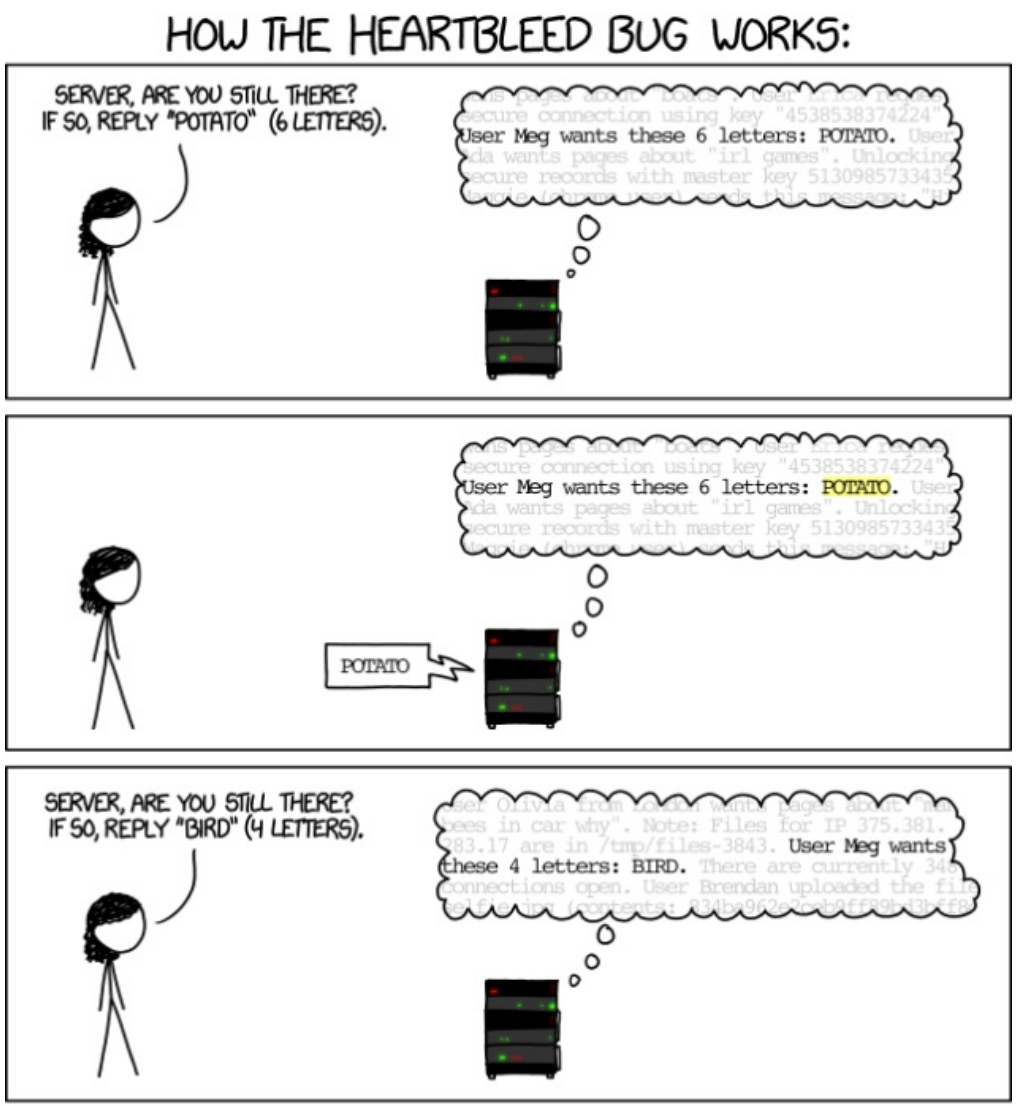
Snowden Leaks

restricted to those specifically indoctrinated for BULLRUN. The various types of security covered by BULLRUN include, but are not limited to, TLS/SSL, https (e.g. webmail), SSH, encrypted chat, VPNs and encrypted VOIP. The specific instances of these technologies that can be exploited will be published in a separate Annexe (available to BULLRUN indoctrinated staff).

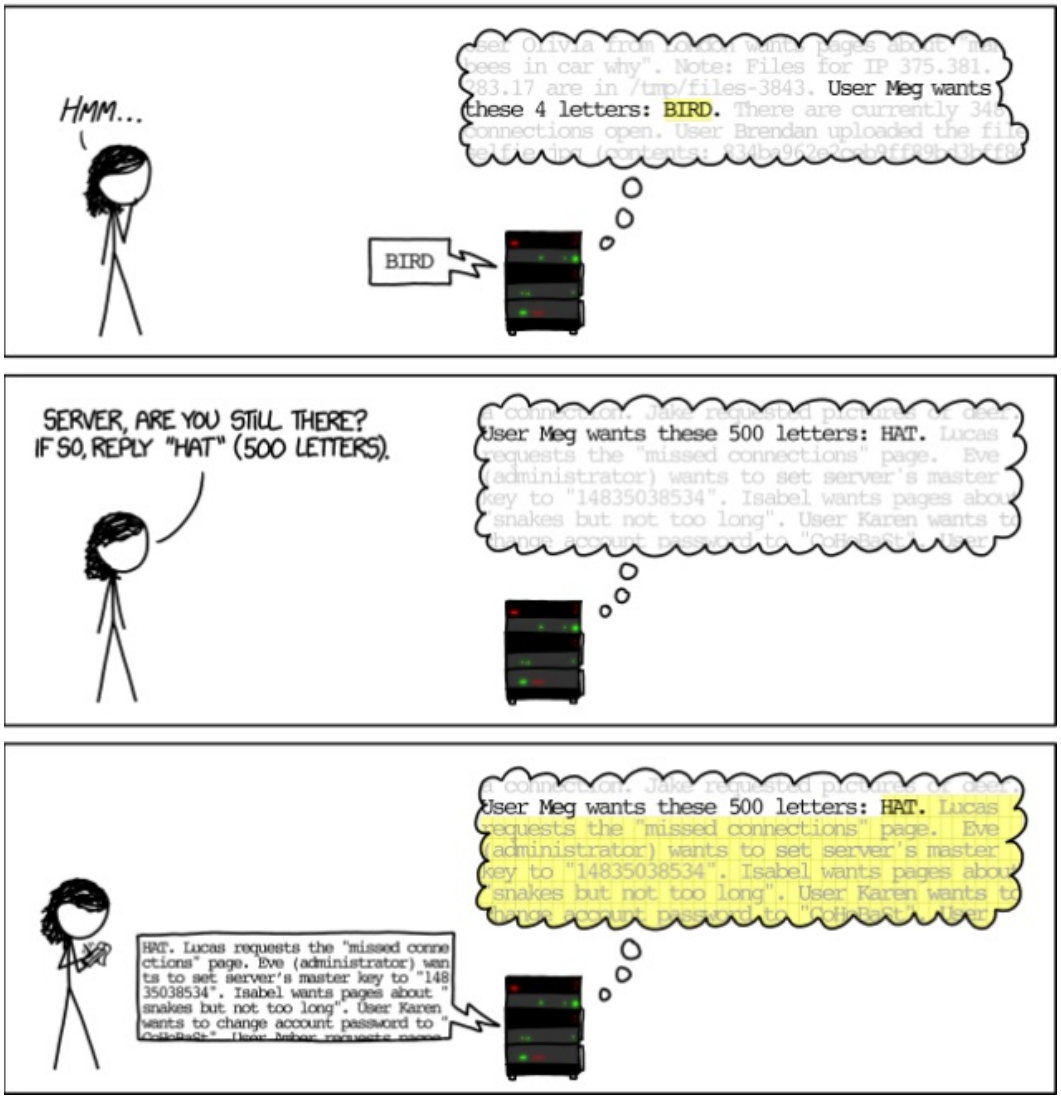
Bazı İddialar

- NSA has been working to systematically influence encryption standards or insert backdoors in the code of commercial encryption software to enable it to access Internet users communications
- the agency has the ability to access a wide range of information stored on smartphones including iPhones, Blackberrys, and those running Googles Android operating system
- $250m-a-year US program works covertly with tech companies to insert weaknesses into products

Heartbeat → Heartbleed



Heartbeat → Heartbleed



Dual EC DRBG

Dual Elliptic Curve Deterministic Random Bit Generator

- Haziran 2004: ANSI X9.82 Dual EC DRBG'yi içeriyor

Dual EC DRBG

Dual Elliptic Curve Deterministic Random Bit Generator

- Haziran 2004: ANSI X9.82 Dual EC DRBG'yi içeriyor
- 2004: RSA Dual EC DRBG'yi varsayılan üreteç olarak belirliyor (Reuters'a göre bunun için NSA $10.000.000 ödüyor)

Dual EC DRBG

Dual Elliptic Curve Deterministic Random Bit Generator

- Haziran 2004: ANSI X9.82 Dual EC DRBG'yi içeriyor
- 2004: RSA Dual EC DRBG'yi varsayılan üreteç olarak belirliyor (Reuters'a göre bunun için NSA $10.000.000 ödüyor)
- 2005: ISO/IEC 18031:2005 standardında yer alıyor

Dual EC DRBG

Dual Elliptic Curve Deterministic Random Bit Generator

- Haziran 2004: ANSI X9.82 Dual EC DRBG'yi içeriyor
- 2004: RSA Dual EC DRBG'yi varsayılan üreteç olarak belirliyor (Reuters'a göre bunun için NSA $10.000.000 ödüyor)
- 2005: ISO/IEC 18031:2005 standardında yer alıyor
- Haziran 2006: NIST standartlarında yer alıyor

Dual EC DRBG

Dual Elliptic Curve Deterministic Random Bit Generator

- Haziran 2004: ANSI X9.82 Dual EC DRBG'yi içeriyor
- 2004: RSA Dual EC DRBG'yi varsayılan üreteç olarak belirliyor (Reuters'a göre bunun için NSA $10.000.000 ödüyor)
- 2005: ISO/IEC 18031:2005 standardında yer alıyor
- Haziran 2006: NIST standartlarında yer alıyor
- Snowden dökümanları NSA'in BULLRUN projesi kapsamında bu algoritmaya arka kapı koyduğu belirtiliyor

Dual EC DRBG

Dual Elliptic Curve Deterministic Random Bit Generator

- Haziran 2004: ANSI X9.82 Dual EC DRBG'yi içeriyor
- 2004: RSA Dual EC DRBG'yi varsayılan üreteç olarak belirliyor (Reuters'a göre bunun için NSA $10.000.000 ödüyor)
- 2005: ISO/IEC 18031:2005 standardında yer alıyor
- Haziran 2006: NIST standartlarında yer alıyor
- Snowden dökümanları NSA'in BULLRUN projesi kapsamında bu algoritmaya arka kapı koyduğu belirtiliyor
- Ağustos 2014: Dual EC DRBG kullanarak SSL/TLS'e arka kapı koymanın mümkün olduğu gösteriliyor (Checkoway *et al.*)

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- 17 Haziran 2010: VirusBlokAda (Beyaz Rusya) İran'lı bir müşterinin bilgisayarı sürekli açılıp

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- 17 Haziran 2010: VirusBlokAda (Beyaz Rusya) İran'lı bir müşterinin bilgisayarı sürekli açılıp
- Windows Explorer LNK dosyası Zero-Day exploit (Kasım 2008) (bu sayede USB disklerden yayılıyor)

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- 17 Haziran 2010: VirusBlokAda (Beyaz Rusya) İran'lı bir müşterinin bilgisayarı sürekli açılıp
- Windows Explorer LNK dosyası Zero-Day exploit (Kasım 2008) (bu sayede USB disklerden yayılıyor)
- Haziran 2009'da ortaya çıkmış ve 3 kez güncellenmiştir. RealTek Semiconductor'ın (Taiwan) geçerli imzalanmış sertifikasına sahip. Otoriteler sertifikayı iptal etti.

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- 17 Haziran 2010: VirusBlokAda (Beyaz Rusya) İran'lı bir müşterinin bilgisayarı sürekli açılıp
- Windows Explorer LNK dosyası Zero-Day exploit (Kasım 2008) (bu sayede USB disklerden yayılıyor)
- Haziran 2009'da ortaya çıkmış ve 3 kez güncellenmiştir. RealTek Semiconductor'ın (Taiwan) geçerli imzalanmış sertifikasına sahip. Otoriteler sertifikayı iptal etti.
- JMicron Technology'nin çalınmış sertifikasını da kullandığı fark edildi (ESET)

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- 17 Haziran 2010: VirusBlokAda (Beyaz Rusya) İran'lı bir müşterinin bilgisayarı sürekli açılıp
- Windows Explorer LNK dosyası Zero-Day exploit (Kasım 2008) (bu sayede USB disklerden yayılıyor)
- Haziran 2009'da ortaya çıkmış ve 3 kez güncellenmiştir. RealTek Semiconductor'ın (Taiwan) geçerli imzalanmış sertifikasına sahip. Otoriteler sertifikayı iptal etti.
- JMicron Technology'nin çalınmış sertifikasını da kullandığı fark edildi (ESET)
- 2 firmanın da merkezleri Taiwan'da aynı ticaret merkezinde

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- 17 Haziran 2010: VirusBlokAda (Beyaz Rusya) İran'lı bir müşterinin bilgisayarı sürekli açılıp
- Windows Explorer LNK dosyası Zero-Day exploit (Kasım 2008) (bu sayede USB disklerden yayılıyor)
- Haziran 2009'da ortaya çıkmış ve 3 kez güncellenmiştir. RealTek Semiconductor'ın (Taiwan) geçerli imzalanmış sertifikasına sahip. Otoriteler sertifikayı iptal etti.
- JMicron Technology'nin çalınmış sertifikasını da kullandığı fark edildi (ESET)
- 2 firmanın da merkezleri Taiwan'da aynı ticaret merkezinde
- Hedef Simatic WinCC Step7 yazılımı: Siemens tarafından geliştirilmiş ve fabrikalardaki motor, vana ve şalterlerin kontrolünü sağlayan yazılım

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- 17 Haziran 2010: VirusBlokAda (Beyaz Rusya) İran'lı bir müşterinin bilgisayarı sürekli açılıp
- Windows Explorer LNK dosyası Zero-Day exploit (Kasım 2008) (bu sayede USB disklerden yayılıyor)
- Haziran 2009'da ortaya çıkmış ve 3 kez güncellenmiştir. RealTek Semiconductor'ın (Taiwan) geçerli imzalanmış sertifikasına sahip. Otoriteler sertifikayı iptal etti.
- JMicron Technology'nin çalınmış sertifikasını da kullandığı fark edildi (ESET)
- 2 firmanın da merkezleri Taiwan'da aynı ticaret merkezinde
- Hedef Simatic WinCC Step7 yazılımı: Siemens tarafından geliştirilmiş ve fabrikalardaki motor, vana ve şalterlerin kontrolünü sağlayan yazılım
- Virüs programları önlemlerini aldı ama Symantec araştırmacıları konuyu kapatmadı (Kaliforniya-Tokyo-Paris)

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Stuxnet kötücül (malicious) kısmını hdd yerine RAM'de tutuyor (bir ilk). Sıradan virüslere göre çok büyük (500KB)

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Stuxnet kötücül (malicious) kısmını hdd yerine RAM'de tutuyor (bir ilk). Sıradan virüslere göre çok büyük (500KB)
- www.mypremierefutbol.com ve www.todaysfutbol.com adreslerine (Malezya ve Danimarka) IP, bilgisayar adı, OS sürümü, Step7 olup olmadığı bilgisi yollanıyor, bu siteler virüsü güncelleyebiliyor

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Stuxnet kötücül (malicious) kısmını hdd yerine RAM'de tutuyor (bir ilk). Sıradan virüslere göre çok büyük (500KB)
- www.mypremierefutbol.com ve www.todaysfutbol.com adreslerine (Malezya ve Danimarka) IP, bilgisayar adı, OS sürümü, Step7 olup olmadığı bilgisi yollanıyor, bu siteler virüsü güncelleyebiliyor
- DNS sağlayıcılar bu siteleri Symantec'e yönlendirdiler (1 haftada 38,000 virüslü bilgisayar, 22,000'i İran'dan, 6,700 Endonezya, 3,700 Hindistan, 400 ABD. Sadece 217'sinde Step7 yüklü)

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Stuxnet kötücül (malicious) kısmını hdd yerine RAM'de tutuyor (bir ilk). Sıradan virüslere göre çok büyük (500KB)
- www.mypremierefutbol.com ve www.todaysfutbol.com adreslerine (Malezya ve Danimarka) IP, bilgisayar adı, OS sürümü, Step7 olup olmadığı bilgisi yollanıyor, bu siteler virüsü güncelleyebiliyor
- DNS sağlayıcılar bu siteleri Symantec'e yönlendirdiler (1 haftada 38,000 virüslü bilgisayar, 22,000'i İran'dan, 6,700 Endonezya, 3,700 Hindistan, 400 ABD. Sadece 217'sinde Step7 yüklü)
- 3 zero-day exploit daha: print spooler (Nisan 2009), Windows keyboard file, Task Scheduler file

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Stuxnet kötücül (malicious) kısmını hdd yerine RAM'de tutuyor (bir ilk). Sıradan virüslere göre çok büyük (500KB)
- www.mypremierefutbol.com ve www.todaysfutbol.com adreslerine (Malezya ve Danimarka) IP, bilgisayar adı, OS sürümü, Step7 olup olmadığı bilgisi yollanıyor, bu siteler virüsü güncelleyebiliyor
- DNS sağlayıcılar bu siteleri Symantec'e yönlendirdiler (1 haftada 38,000 virüslü bilgisayar, 22,000'i İran'dan, 6,700 Endonezya, 3,700 Hindistan, 400 ABD. Sadece 217'sinde Step7 yüklü)
- 3 zero-day exploit daha: print spooler (Nisan 2009), Windows keyboard file, Task Scheduler file
- Stuxnet Siemens'in Step7 yazılımındaki varsayılan şifreyi kullanarak (hard-coded, Nisan 2008), bulaştığı bilgisayarın serverın'daki veritabanını kullanarak sistemdeki diğer bilgisayarlara bulaşıyor

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Stuxnet kötücül (malicious) kısmını hdd yerine RAM'de tutuyor (bir ilk). Sıradan virüslere göre çok büyük (500KB)
- www.mypremierefutbol.com ve www.todaysfutbol.com adreslerine (Malezya ve Danimarka) IP, bilgisayar adı, OS sürümü, Step7 olup olmadığı bilgisi yollanıyor, bu siteler virüsü güncelleyebiliyor
- DNS sağlayıcılar bu siteleri Symantec'e yönlendirdiler (1 haftada 38,000 virüslü bilgisayar, 22,000'i İran'dan, 6,700 Endonezya, 3,700 Hindistan, 400 ABD. Sadece 217'sinde Step7 yüklü)
- 3 zero-day exploit daha: print spooler (Nisan 2009), Windows keyboard file, Task Scheduler file
- Stuxnet Siemens'in Step7 yazılımındaki varsayılan şifreyi kullanarak (hard-coded, Nisan 2008), bulaştığı bilgisayarın serverın'daki veritabanını kullanarak sistemdeki diğer bilgisayarlara bulaşıyor
- Virüsün sadece USB belleklerle yayılması, hedefin internete bağlı olmadığı izlenimini uyandırıyor

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Stuxnet'in hangi domain'lere hangi tarihte bulaştığı incelenerek hedefin İran'daki 5 firma olduğu gözlemlendi (ama zero-day exploit'ler nedeniyle bu firmaların dışına taştı)

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Stuxnet'in hangi domain'lere hangi tarihte bulaştığı incelenerek hedefin İran'daki 5 firma olduğu gözlemlendi (ama zero-day exploit'ler nedeniyle bu firmaların dışına taştı)
- Stuxnet kendini 24 Haziran 2012'den sonra kapatıyor (bu tarihe kadar hedefine ulaşacağı düşünülmüş olabilir)

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Stuxnet'in hangi domain'lere hangi tarihte bulaştığı incelenerek hedefin İran'daki 5 firma olduğu gözlemlendi (ama zero-day exploit'ler nedeniyle bu firmaların dışına taştı)
- Stuxnet kendini 24 Haziran 2012'den sonra kapatıyor (bu tarihe kadar hedefine ulaşacağı düşünülmüş olabilir)
- Step7 yüklüyse DLL dosyasını RAM'e kopyalıyor, PLC cihazlarına komutlar yolluyor ve raporlar kendini siliyor (PLC cihazları STL programlama dilini kullanıyor)

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Stuxnet'in hangi domain'lere hangi tarihte bulaştığı incelenerek hedefin İran'daki 5 firma olduğu gözlemlendi (ama zero-day exploit'ler nedeniyle bu firmaların dışına taştı)
- Stuxnet kendini 24 Haziran 2012'den sonra kapatıyor (bu tarihe kadar hedefine ulaşacağı düşünülmüş olabilir)
- Step7 yüklüyse DLL dosyasını RAM'e kopyalıyor, PLC cihazlarına komutlar yolluyor ve raporlar kendini siliyor (PLC cihazları STL programlama dilini kullanıyor)
- Stuxnet normalde 1,064Hz hızla çalışan sistemi 15 dakikalığına 1,410Hz'e çıkartıyor ve 27 gün sonra 50 dakikalığına 2Hz'e indiriyor

Stuxnet, Haziran 2009 (World's First Digital Weapon)

İran Cumhurbaşkanı Mahmoud Ahmadinejad Natanz Nükleer Tesisi santrifuj turundayken (2008)

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Temmuz 2009: Wikileaks İran'ın Natanz Nükleer Tesisinde nükleer bir kaza olduğunu ve İran Atom Enerjisi Orgnizasyonu Başkanı'nın istifa ettiğini duyurdu

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Temmuz 2009: Wikileaks İran'ın Natanz Nükleer Tesisinde nükleer bir kaza olduğunu ve İran Atom Enerjisi Orgnizasyonu Başkanı'nın istifa ettiğini duyurdu
- Normalde İran yılda 800 santrifüjü değiştiriyordu. Stuxnet'ten sonra bu sayı 1-2 ayda 2000'e yükseldi.

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Temmuz 2009: Wikileaks İran'ın Natanz Nükleer Tesisinde nükleer bir kaza olduğunu ve İran Atom Enerjisi Orgnizasyonu Başkanı'nın istifa ettiğini duyurdu
- Normalde İran yılda 800 santrifüjü değiştiriyordu. Stuxnet'ten sonra bu sayı 1-2 ayda 2000'e yükseldi.
- Symantec Stuxnet hakkındaki bilgileri paylaştıktan 2 hafta sonra Tahran'da 2 nükleer enerji mühendisi aynı anda 2 motosikletli saldırgan tarafından bombalı saldırı sonucu ölüdürüldü

Stuxnet, Haziran 2009 (World's First Digital Weapon)

Stuxnet

- Temmuz 2009: Wikileaks İran'ın Natanz Nükleer Tesisinde nükleer bir kaza olduğunu ve İran Atom Enerjisi Orgnizasyonu Başkanı'nın istifa ettiğini duyurdu
- Normalde İran yılda 800 santrifüjü değiştiriyordu. Stuxnet'ten sonra bu sayı 1-2 ayda 2000'e yükseldi.
- Symantec Stuxnet hakkındaki bilgileri paylaştıktan 2 hafta sonra Tahran'da 2 nükleer enerji mühendisi aynı anda 2 motosikletli saldırgan tarafından bombalı saldırı sonucu ölüdürüldü
- Stuxnet'in Amerikan-İsrail ortak yapımı olduğu düşünülüyor

Regin (The Most Sophisticated Spy Tool Yet)

Regin

- 2011 yılında Avrupa Komisyonu Hack'lendi (zero-day exploit), (2010 tarihli Snowden dökümanları NSA'in Avrupa Komisyonu'nu hacklemeyi hedeflediğini gösteriyor)

Regin (The Most Sophisticated Spy Tool Yet)

Regin

- 2011 yılında Avrupa Komisyonu Hack'lendi (zero-day exploit), (2010 tarihli Snowden dökümanları NSA'in Avrupa Komisyonu'nu hacklemeyi hedeflediğini gösteriyor)
- 2013 yılında Belgacom (Belçika GSM firması): Snowden dökümanları Belgacom adminlerinin parolalarının çalındığını ve bu şekilde GSM operatörünün kontrolünün ele geçirildiğini söylüyor

Regin (The Most Sophisticated Spy Tool Yet)

Regin

- 2011 yılında Avrupa Komisyonu Hack'lendi (zero-day exploit), (2010 tarihli Snowden dökümanları NSA'in Avrupa Komisyonu'nu hacklemeyi hedeflediğini gösteriyor)
- 2013 yılında Belgacom (Belçika GSM firması): Snowden dökümanları Belgacom adminlerinin parolalarının çalındığını ve bu şekilde GSM operatörünün kontrolünün ele geçirildiğini söylüyor
- Kaspersky aynı saldırının bir Ortadoğu ülkesine de yapıldığını ve GSM operatörünün ele geçirildiğini iddia ediyor (büyük olasılıkla Afganistan)

Regin (The Most Sophisticated Spy Tool Yet)

Regin

- 2011 yılında Avrupa Komisyonu Hack'lendi (zero-day exploit), (2010 tarihli Snowden dökümanları NSA'in Avrupa Komisyonu'nu hacklemeyi hedeflediğini gösteriyor)
- 2013 yılında Belgacom (Belçika GSM firması): Snowden dökümanları Belgacom adminlerinin parolalarının çalındığını ve bu şekilde GSM operatörünün kontrolünün ele geçirildiğini söylüyor
- Kaspersky aynı saldırının bir Ortadoğu ülkesine de yapıldığını ve GSM operatörünün ele geçirildiğini iddia ediyor (büyük olasılıkla Afganistan)
- 5 ay sonra Belçikalı kriptograf Jean-Jacques Quisquater aynı saldırıya maruz kaldı

Regin (The Most Sophisticated Spy Tool Yet)

Regin

- 2011 yılında Avrupa Komisyonu Hack'lendi (zero-day exploit), (2010 tarihli Snowden dökümanları NSA'in Avrupa Komisyonu'nu hacklemeyi hedeflediğini gösteriyor)
- 2013 yılında Belgacom (Belçika GSM firması): Snowden dökümanları Belgacom adminlerinin parolalarının çalındığını ve bu şekilde GSM operatörünün kontrolünün ele geçirildiğini söylüyor
- Kaspersky aynı saldırının bir Ortadoğu ülkesine de yapıldığını ve GSM operatörünün ele geçirildiğini iddia ediyor (büyük olasılıkla Afganistan)
- 5 ay sonra Belçikalı kriptograf Jean-Jacques Quisquater aynı saldırıya maruz kaldı
- 2014 Kasım: Cihangir Tezcan :)

Regin (The Most Sophisticated Spy Tool Yet)

Regin

- 2011 yılında Avrupa Komisyonu Hack'lendi (zero-day exploit), (2010 tarihli Snowden dökümanları NSA'in Avrupa Komisyonu'nu hacklemeyi hedeflediğini gösteriyor)
- 2013 yılında Belgacom (Belçika GSM firması): Snowden dökümanları Belgacom adminlerinin parolalarının çalındığını ve bu şekilde GSM operatörünün kontrolünün ele geçirildiğini söylüyor
- Kaspersky aynı saldırının bir Ortadoğu ülkesine de yapıldığını ve GSM operatörünün ele geçirildiğini iddia ediyor (büyük olasılıkla Afganistan)
- 5 ay sonra Belçikalı kriptograf Jean-Jacques Quisquater aynı saldırıya maruz kaldı
- 2014 Kasım: Cihangir Tezcan :)
- Regin tahminen 2008'den beri ortalıkta ve tüm ağı ve altyapısını ele geçirmek üzere tasarlanmış (büyük olasılıkla NSA ve GCHQ)

Regin (The Most Sophisticated Spy Tool Yet)

Regin

Regin özellikleri:

- Remote access trojan
- keystroke logger
- clip board sniffer
- password sniffer
- collect information about USB devices
- email extraction module
- scan and retrieve deleted files

Teşekkürler

Teşekkürler