Budapest University of Technology and Economics

A kriptográfia története tömören – a szkütalétól az SSL-ig

Dr. Buttyán Levente
Laboratory of Cryptography and System Security (CrySyS)
Department of Telecommunications
Budapest University of Technology and Economics
buttyan@crysys.hu

www.crysys.hu

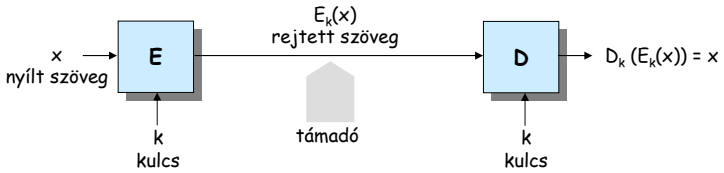
A kommunikáció biztonsága

- főbb biztonsági követelmények
  - adatok titkossága
  - adatok integritásának védelme
  - adatok hitelességének biztosítása
  - üzenet küldésének és vételének letagadhatatlansága
  - a rendszer erőforrásaihoz való hozzáférés korlátozása
- a biztonság három pillére
  - fizikai védelem
  - algoritmikus védelem
  - humán oldal (rendszabályok, nevelés, stb.)
- a kriptográfia az algoritmikus védelem elmélete

A kriptográfia története

- a 20. század második feléig a kriptográfiát kizárólag katonai és diplomáciai alkalmazásokban használták
  - kriptgráfia = titkosírás, rejtjelezés
- a 20. század második felétől a kriptográfia megjelent az üzleti életben (elsősorban banki alkalmazásokban)
  - a titkosság mellett fontossá vált az integritásvédelem, a hitelesítés, a letagadhatatlanság, stb.
- a 20. század végétől a kriptográfia a mindennapi élet részévé vált
  - SSL (Secure Socket Layer) – Web tranzakciók biztonsága
  - GSM biztonsági architektúra – mobiltelefon-hálózat biztonsága

A (szimmetrikus) rejtjelezés klasszikus modellje



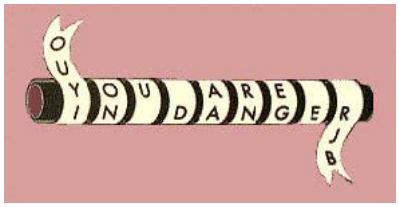
- a támadó célja
  - a rejtett szövegek szisztematikus megfejtése
  - a kulcs megfejtése
- a Kerkchoff-elv
  - a támadó pontosan ismeri a kódoló és a dekódoló transzformáció működését
  - a támadó nem ismeri a kulcsot

Történelmi példák

- „már az ókori görögök is …" – a spártaiak szkütaléja
- „veni, vidi, vici" – Julius Caesar rejtjelezője
- a „feltörhetetlen" sifre – Vigenère kód
- a rejtjelezés gépesítése – az Enigma

A szkütalé

- i.e. 400 körül használták a spártaiak
- az üzenet betűinek átrendezésén alapszik
- kulcs = a rúd átmérője
  kulcstér mérete kicsi



Julius Caesar rejtjelezője

- az üzenet betűinek helyettesítésén alapszik
- minden betűt az ABC-ben hárommal későbbi betűvel helyettesítünk
  - nyílt: 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
  - kódolt: 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

RETURN TO ROME → UHWXUA WR URPH

- kulcs = az eltolás mértéke (Caesar esetén 3)
  kulcstér mérete = 26-1 = 25

Monoalfabetikus helyettesítés

- a Caesar rejtjelező általánosítása
- kód ABC = nyílt ABC permutációja
  - nyílt: 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
  - kódolt: T Q L R B W J G F Y N C P E K S D U V I X M Z A H O
- kulcs = az alkalmazott permutáció
  kulcstér mérete = 26! ~ $1.56*2^{88}$

Nagy számok

a következő jégkorszakig hátralevő idő..... 2^{39} sec
a Nap szupernovává válásáig hátrlevő idő..... 2^{55} sec
a Föld kora ..... 2^{55} sec
az Univerzum kora ..... 2^{59} sec

a Földön található atomok száma..... 2^{170}
a Napban található atomok száma ..... 2^{190}
a galaxisunkban található atomok száma..... 2^{223}
az Univerzumban található atomok száma..... 2^{265}
(sötét anyag nélkül)

az Univerzum térfogata ..... 2^{280} cm^3

(forrás: Schneier, Applied Cryptography, 2nd ed., Wiley 1996)

A monoalfabetikus helyettesítés feltörése

- minden nyelvnek sajátos betűstatisztikája van
  - egy átlagos szövegben nem minden betű fordul elő azonos valószínűséggel
  - vannak kimagaslóan gyakori betűk
    az angolban például:
    e – 12.7%
    t – 9.1%
  - és kirívóan ritkák
    az angolban például:
    z – 0.1%
    j – 0.2%
- monoalfabetikus helyettesítés esetén a rejtett szöveg megőrzi az eredeti szöveg betűstatisztikáját (!)
  - leggyakrabban előforduló betű nagy valószínűséggel az „e" vagy a „t" kódoltja
  - néhány betű megfejtése után a rejtett szöveg dekódolása általában egyszerű

Polialfabetikus helyettesítés – a Vigenère kód

	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

kódolás:

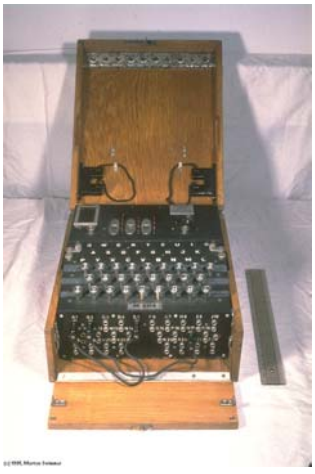
```
        kulcs: RELAT IONSR ELATI ONSRE LATIO NSREL
  nyílt szöveg: TOBEO RNOTT OBETH ATIST HEQUE STION
rejtett szöveg: KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY
```

dekódolás:

```
        kulcs: RELAT IONSR ELATI ONSRE LATIO NSREL
rejtett szöveg: KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY
  nyílt szöveg: TOBEO RNOTT OBETH ATIST HEQUE STION
```


Az Enigma

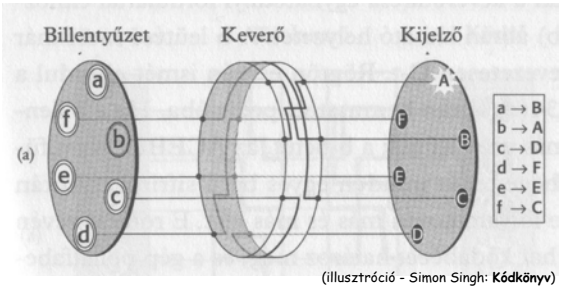
- az első elektromechanikus rejtjelező gép
- Arthur Scherbius szabadalma [1918]
- 1926-ban rendszeresítik a német hadseregben



Az Enigma működési elve

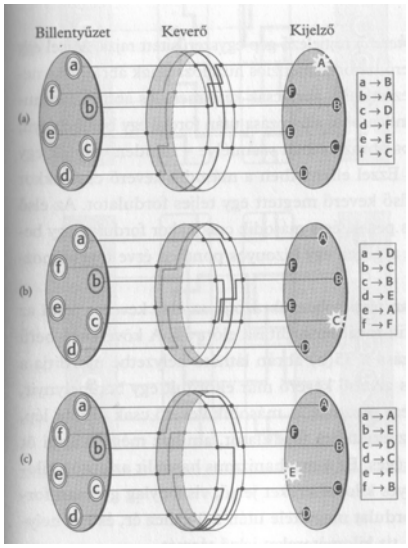
- három fő egység:
  - billentyűzet – nyílt / rejtett szöveg bevitele
  - kijelzőpanel – rejtett / nyílt szöveg kijelzése
  - keverőegység – rejtett szöveg előállítása / nyílt szöveg visszaállítása

- az Enigma lelke a keverőtárcsa (rotor)



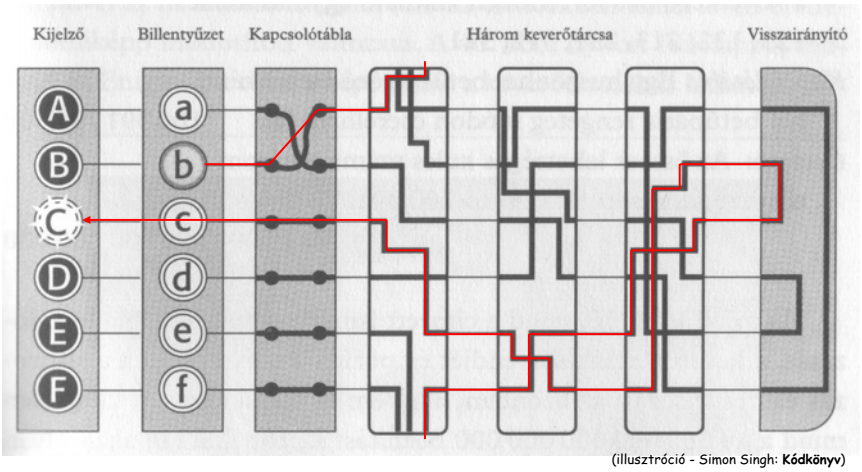
(illusztráció - Simon Singh: **Kódkönyv**)

Az Enigma működési elve



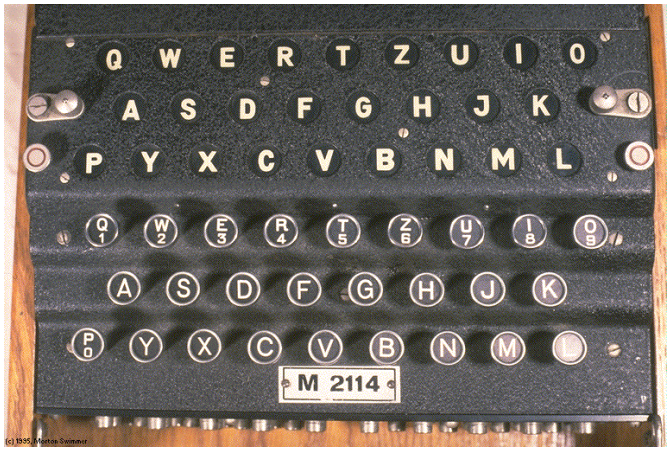
(illusztráció - Simon Singh: **Kódkönyv**)

Az Enigma működési elve

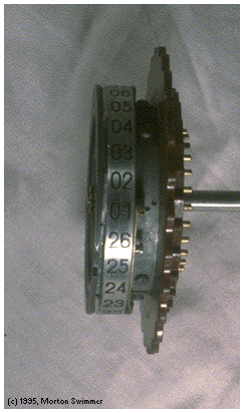


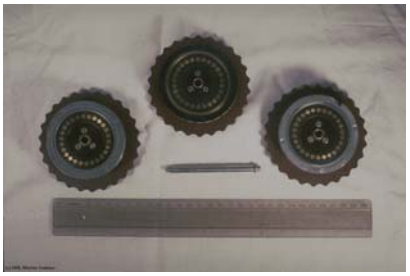
(illusztráció - Simon Singh: **Kódkönyv**)

Enigma – a billentyűzet és a kijelzőpanel

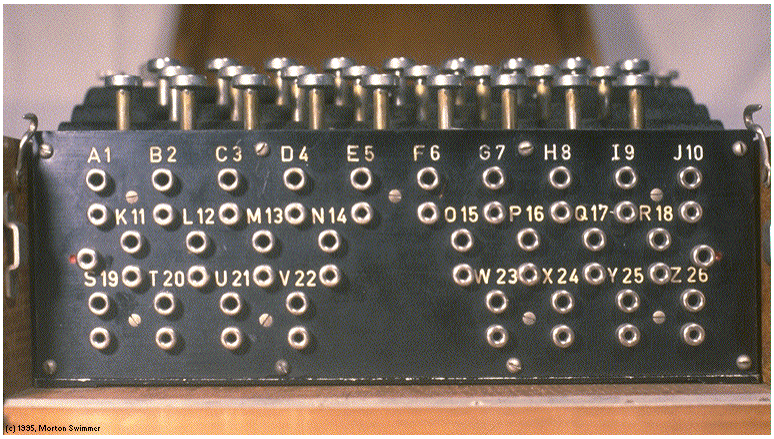


Enigma – a keverőtárcsák





Enigma – a kapcsolótábla



Az Enigma használata

- alapbeállítás
  - kapcsolótábla beállítása (pl: A/L – P/R – T/D – B/W – K/F – O/Y)
  - keverőtárcsák sorrendje (pl: II – III - I)
  - keverőtárcsák beállítása (pl: Q – C - W)

  (a kulcstér mérete = 100391791500 x 6 x 26^3 ~ 10^{16} ~ 2^{53})

- nyílt szöveg bevitele a billentyűzeten

- rejtett szöveg leolvasása a kijelző panelről

Az Enigma feltörése

Marian Rejewski
lengyel matematikus

- Hans-Thilo Schmidt német kém 10 ezer márkáért eladja a katonai Engima használati útmutatóit a franciáknak [1931. november 8.]

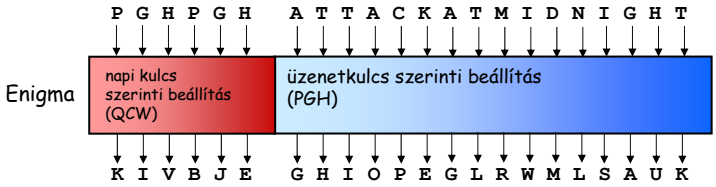
- ezek segítségével a szövetségesek megépítik a katonai Engima mását

- a franciák feltörhetetlennek tartják az Enigmát, s átadják az összes dokumentumot a lengyeleknek

- a lengyel Biuro Szyfrów felvesz húsz fiatal matematikust a poznani egyetemről, majd kiválasztja közülük a három legtehetségesebbet; köztük a 23 éves Marian Rejewskit

Az Enigma feltörése

- a németek nem a napi kulccsal rejtjelezték üzeneteiket
  - ha a napi kulcsot használták volna, akkor több ezer üzenetet kódoltak volna ugyanazzal a kulccsal, és ez növelte volna a napi kulcs megfejtésének esélyét
- helyette minden üzenetet egy egyszeri üzenetkulccsal rejtjeleztek, majd az üzenetkulcsot a napi kulccsal kódolták, és a kódolt kulcsot a rejtjelezett üzenet elé csatolták
  - üzenetkulcs: a kapcsolótábla beállítása és a keverőtárcsák sorrendje megegyezett a napi kulcséval, a keverőtárcsák beállítása véletlen
- valójában az üzenetkulcsot kétszer gépelték be az Enigmába, hogy a kulcs átvitele során keletkező hibákat detektálni tudják
- példa:



Az Enigma feltörése

- Rejewski megérezte, hogy az üzenetkulcs ismétlése a gyenge pont
- egy év alatt kidolgozott egy módszert a napi kulcs megfejtésére
- sőt, gépesítette a kulcs megfejtését
  - egy módosított Enigma folyamatosan változtatta a keverőtárcsák beállítását, míg rá nem akadt a helyes beállításra
  - 6 gép dolgozott párhuzamosan (6 lehetséges keverőtárcsa sorrend)
  - a gépet zakatolása miatt *időzített bombának* hívta
- a lengyelek 1933-tól rutinszerűen fejtették meg a németek üzeneteit

Az Enigma feltörése

- 1938 decemberében a németek fokozzák az Enigma biztonságát
  - 2 új keverőtárcsát rendszeresítettek (6-ról 60-ra ugrott a lehetséges keverőtárcsa sorrendek száma)
  - 6-ról 10-re növelték a betűcserék számát a kapcsolótáblán
  - ezzel $1.59*10^{20}$-ra emelkedett a kulcstér mérete
- Hitler felbontja a Lengyelországgal kötött megnemtámadási szerződést [1939. április 27.]
- a lengyelek felfedik eredményeiket a szövetségeseknek [1939. július 24.]
- a bombák tervrajzát eljuttatják Londonba [1939. augusztus 16.]
- Németország lerohanja Lengyelországot [1939. szeptember 1.]

Az Enigma feltörése

Ridley kapitány vadászata a Bletchley Parkban
[1939. augusztus]

Az Enigma feltörése

- a britek tökéletesítik a bombát, és további leleményes ötletekkel állnak elő
  - cilly-k
    - a német Enigma kezelők a csata hevében gyakran nagyon egyszerű üzenetkulcsokat választottak (pl. QWE, BNM)
    - egy Enigma kezelő rendszeresen barátnője monogramját használta üzenetkulcsnak (C.I.L.)
    - az ilyen gyenge üzenetkulcsokat *cilly*-knek hívták (~silly)
  - keverőtárcsákra vonatkozó megkötések
    - a németek minden nap változtatták a keverőtárcsák sorrendjét
    - egyetlen tárcsa sem maradhatott egy helyen kétszer egymás után
    - pl. I-II-V után nem jöhetett III-II-IV
    - ez az óvintézkedés csökkentette a számba jöhető keverőtárcsa sorrendeket, és így könnyítette a britek dolgát
    - hasonlóképpen, a kapcsolótáblán sem lehett szomszédos betűket felcserélni

Az Enigma feltörése

Alan Turing
brit matematikus

- Alan Turing csatlakozik a Bletchley parki kriptográfusokhoz [1939. szeptember 4.]
  - bár csak 27 éves, ekkor már híres matematikus, túl van a Turing-gép megalkotásán
- feladata egy új kulcsfejtési eljárás kidolgozása, mely nem használja ki az ismétlődő üzenetkulcsot az üzenet elején
- Turing megoldja a feladatot, módszere az ún. *támpontokra* épül
  - a németek precízek és jól szervezettek
  - üzeneteik szabályos, kiszámítható struktúrájúak
  - egy-egy szó könnyen megsejthető
  - pl. minden este 6-kor időjárásjelentést küldtek, mely jól meghatározott helyen tartalmazta az "időjárás" (wetter) szót
- Turing tervei alapján új bombákat építenek (Victory, Agnus Dei) [1940. március - augusztus]
- a németek megváltoztatják kulcscsere eljárásukat [1940. május 1.]

Az Enigma feltörése

- a Bletchley Park teljesítménye a szövetségesek győzelmének döntő tényezője volt
- történészek becslése szerint az Enigma feltörése nélkül a háború akár 1948-ig is eltarthatott volna !
- a háború után a bombákat szétszedték, a dokumentumokat pedig elégették
- a Bletchley parki kriptográfusok visszatértek a civil életbe (titoktartás mellett)
- a titoktartást 1970-ben oldották fel, és a világ ekkor szerzett csak tudomást a Bletchley Park létezéséről és az Enigma feltöréséről
- Alan Turing 1954. június 7-én öngyilkos lett

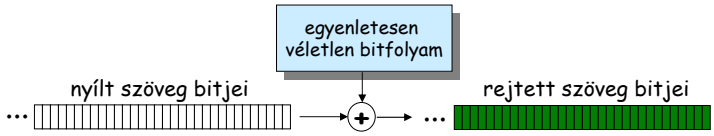
Egy valóban feltörhetetlen rejtjelező – a one-time pad

- mod 2 összeadás $\oplus$: $a \oplus b = (a + b) \bmod 2$

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

- a mod 2 összeadás tulajdonságai:
  1. $x \oplus x = 0$
  2. $x \oplus 0 = x$

A one-time pad működése



- kódolás
  - $y_i = x_i \oplus k_i$
  - ahol x_i a nyílt szöveg i. bitje, y_i a rejtett szöveg i. bitje
  - k_i az egyenletes eloszlású véletlen kulcsfolyam i. bitje
- dekódolás
  - $x_i = y_i \oplus k_i = x_i \oplus k_i \oplus k_i = x_i$

A one-time pad tökéletessége

- tegyük fel, hogy a támadó megfigyeli az Y rejtett szöveget
- mivel minden kulcs egyformán valószínű, ezért minden nyílt szöveg egyforma valószínűséggel lehetséges
- Claude Shannon [1949] bebizonyította, hogy

$$I(X; Y) = H(X) - H(X|Y) = 0$$

- Shannon megadta a tökéletesség szükséges feltételét is:

$$H(K) \geq H(X)$$

ami praktikusan azt jelenti, hogy a kulcs mérete nem lehet kisebb, mint a (tömörített) nyílt szöveg mérete

Modern kriptográfia

- a one-time pad tökéletes, de hatalmas kulcsmérete miatt nem praktikus
- a gyakorlatban nincs szükség elméletileg feltörhetetlen rejtjelezőre, elegendő, ha a rejtjelező praktikusan feltörhetetlen (a mai technológia mellett irdatlan hosszú ideig tart feltörni)
- két jól ismert példa:
  - DES (Data Encryption Standard)
  - RSA (Rivest-Shamir-Adleman)

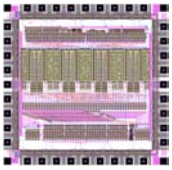
Shannon tervezési ötlete

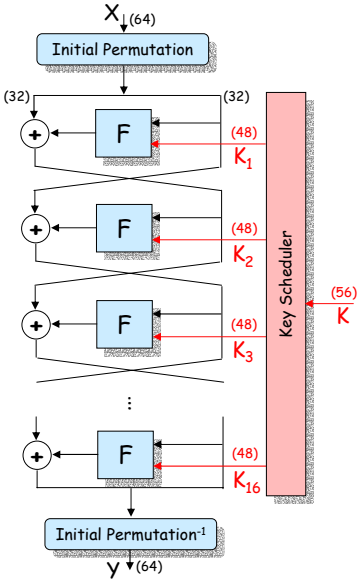
Claude E. Shannon

- készítsünk komplex rejtjelezőt egyszerű transzformációk egymás után többszöri alkalmazásával
- az egyszerű transzformációk egyike sem elegendő önmagában, de egymást kiegészítve már megfelelő védelmet nyújthatnak
- alkalmazható egyszerű transzformációk pl:
  - kis méretű helyettesítések (táblázatban tárolható)
  - nagy méretű bit-permutációk (HW-ben könnyen implementálható)

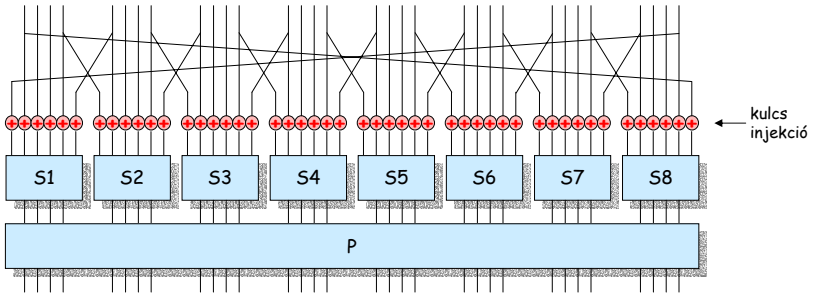
A DES

- az IBM fejlesztette ki a 70-es években Lucifer néven
- szimmetrikus kulcsú blokkrejtjelező
- jellemzők:
  - Feistel struktúra (kódoló és dekódoló séma megegyezik)
  - rétegek száma: 16
  - bemenet mérete: 64 bit
  - kimenet mérete: 64 bit
  - kulcs mérete: 56





A DES



- Si – substitution box (S-box)
- P – permutation box (P-box)

A DES támadása

- lineáris kriptanalízis (LC)
  - a ma ismert legerősebb támadás a DES ellen
  - irdatlan mennyiségű (~2^{43}) ismert nyílt szöveg – rejtett szöveg párra van szükség hozzá → praktikusan kivitelezhetetlen támadás
- differenciális kriptanalízis (DC)
  - általános támadás iteratív blokk rejtjelezők ellen (pl. DES, FEAL, IDEA)
  - alapvetően választott nyílt szövegű támadás
  - DES esetén, ~2^{47} választott nyílt szövegre (és hozzátartozó rejtett szövegre) van szükség hozzá → praktikusan kivitelezhetetlen támadás
- a DES-t DC ellen optimalizálták a tervezés során
- LC ellen növelni lehet az ellenállóképességét (úgy látszik a DES tervezői nem tudtak az LC lehetőségéről)

Új fejezet a kritpográfia történetében

- Whitfield Diffie és Martin Hellman:
  New Directions in Cryptography
  IEEE Transactions on Information Theory, 1976

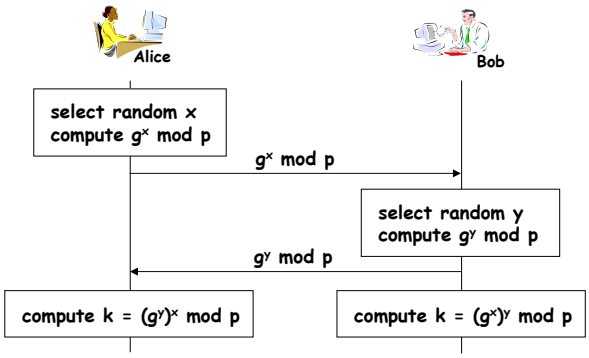
Raplh Merkle, Martin Hellman, és Whitfield Diffie

Diszkrét hatványozás mint egyirányú függvény

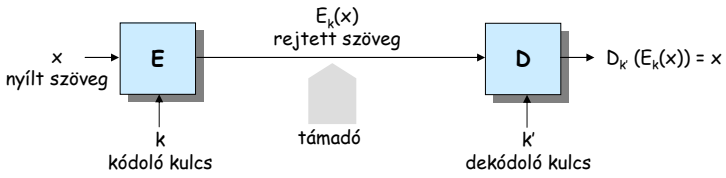
- adott egy p prím
- $Z_p^* = \{1, 2, \ldots, p-1\}$
- g a Z_p^* egy generátora
  - $Z_p^* = \{g^0 \bmod p, g^1 \bmod p, \ldots, g^{p-2} \bmod p\}$
- $f(x) = g^x \bmod p$
  - ha adott x, akkor f(x)-et könnyű kiszámítani
  - ha adott y = f(x), akkor x-et nehéz meghatározni (diszkrét log probléma)
- példa:
  - $p = 7$, $Z_7^* = \{1, 2, 3, 4, 5, 6\}$, $g = 3$
  - $3^0 = 1$, $3^1 = 3$, $3^2 = 9 = 2$, $3^3 = 27 = 6$, $3^4 = 81 = 4$, $3^5 = 243 = 5$
- miért egyirányú a diszkrét hatványozás?
  - $453^x \bmod 21\,997 = 5789$, határozzuk meg x-et!

A Diffie-Hellman-Merkle kulcscsere protokoll

feltevés: adott egy p prím és a $Z_p^* = \{1, 2, \ldots, p-1\}$ egy g generátora



Az aszimmetrikus kulcsú kriptográfia modellje



- aszimmetrikus kulcsok
  - k' kiszámítása k-ból nehéz feladat (NP)
  - k-t nyilvánosságra lehet hozni (nyilvános kulcsú kriptográfia)
- a nyilvános kulcs nem titkos, de a hitelességét biztosítani kell !
- erre a ma ismert legelterjedtebb módszer a kulcstanusitványok használata (PKI)

Az RSA algoritmus

- Ronald Rivest, Adi Shamir, és Leonard Adleman,
  A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, 1978


Ronald Rivest


Adi Shamir


Leonard Adleman

Az RSA algoritmus

- kulcs generálás
  - válasszunk két nagy prímet, p-t és q-t (mindkettő kb. 500 bites)
  - $n = pq$, $\phi(n) = (p-1)(q-1)$
  - válasszunk egy e számot, melyre $1 < e < \phi(n)$ és lnko(e, $\phi(n)$) = 1
  - számítsuk ki e inverzét mod $\phi(n)$, azaz azt a d-t, melyre ed mod $\phi(n) = 1$ (p és q ismeretében ez nem nehéz feladat)
  - a nyilvános kulcs (e, n)
  - a privát kulcs d
- kódolás
  - a nyílt üzenetet egy $m \in [0, n-1]$ egész számként reprezentáljuk
  - a rejtett üzenet számítása: $c = m^e \bmod n$
- dekódolás
  - a nyílt üzenet számítása: $m = c^d \bmod n$

Az RSA algoritmus egy példán keresztül

- legyen p = 73, q = 151
- n = 73*151 = 11023
- $\phi(n)$ = 72*150 = 10800
- legyen e = 11 [lnko(11, 10800) = 1, mert $10800 = 2^4*3*5^2*9$]
- d-t az euklideszi algoritmussal számoljuk: d = 5891

- tegyük fel, hogy m = 17
- $c = 17^{11} \bmod 11023 = 1782$
- $m = 1782^{5891} \bmod 11023$
- négyzetre emelés és szorzás módszere:

$5891 = 2^0 + 2^1 + 2^8 + 2^9 + 2^{10} + 2^{12}$

$1782^{5891} = 1782^{2^{12}} * 1782^{2^{10}} * 1782^{2^9} * 1782^{2^8} * 1782^{2^2} * 1782 =$

$= (\ldots ((1782^2)^2)^2 \ldots)^2 * (\ldots ((1782^2)^2)^2 \ldots)^2 * \ldots$

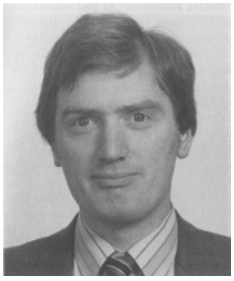
$= 17 \pmod{11023}$

Az RSA biztonsága

- az egész számok faktorizációja jól ismert nehéznek vélt feladat
  - adott egy n pozitív egész, keressük n prím faktorait
    - igazi komplexitása nem ismert
    - úgy sejtik, hogy nem P-beli (nincs rá hatékony megoldás)
- d kiszámítása (e, n)-ből ekvivalens n faktorizálásával
- úgy sejtik, hogy m kiszámítása c-ből és (e, n)-ből (RSA probléma) ekvivalens n faktorizálásával
  - ha n faktorai ismertek, akkor (e,n)-ből könnyen kiszámolható d, majd ennek segítségével c-ből m
  - a másik irányra nincs formális bizonyítás

A nyilvános kulcsú kriptográfia titkos története

James Ellis



Clifford Cocks

Malcolm Williamson

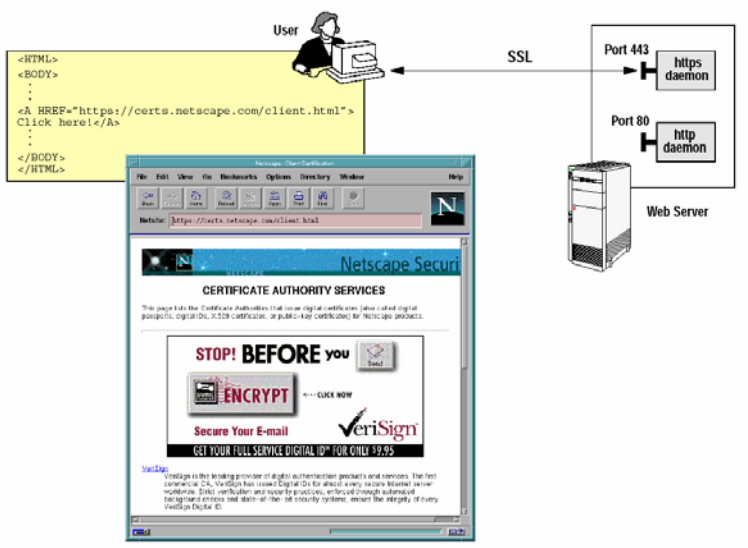
A nyilvános kulcsú kriptográfia titkos története

- Ellis, Cocks, és Williamson a brit titkosszolgálat emberei voltak
- 1969-ben Ellis rájött, hogy nyilvános kulcsú kriptográfia lehetséges (ő nem-titkos kódolásnak nevezte)
  - kidolgozta a publikus és privát kulcsok elméletét
  - tudta, hogy kell valamilyen egyirányú függvény, amely csak akkor válik megfordíthatóvá, ha a címzett birtokában van egy bizonyos információnak
- 1973-ban Cocks kitalálta a később RSA néven ismertté vált kódolást
  - röviddel belépése után, Cocksnak elmondták a problémát
  - még aznap este, fél óra alatt kidolgozta az RSA kódot
  - számelmélettel foglalkozott, és azonnal a faktorizációra gondolt, mint egyirányú függvény
- 1974-ben Williamson (Cocks barátja) felfedezi a később Diffie-Hellman kulcscsere néven ismertté vált eljárást
- 1975-re Ellis, Cocks, és Williamson a nyilvános kulcsú kriptográfia összes alapvető tételét kidolgozta – de hallgatniuk kellett (1997-ig)

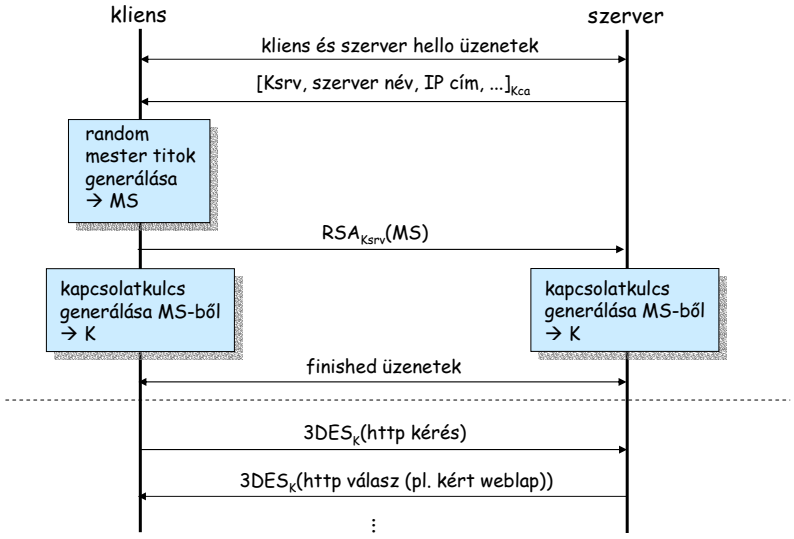
Az SSL protokoll

- a Netscape fejlesztette ki a 90-es évek közepén
- célja biztonságos kapcsolat létrehozása két távoli (TCP) alkalmazás között
- tipikusan: biztonságos kapcsolat létrehozása egy web szerver és egy web böngésző között
- az SSL 3.0 de facto szabvánnyá vált az Interneten
- az SSL 3.1-es verziója TLS néven hivatalos Internet szabvány lett

Az SSL működése



Az SSL működése (egyszerűsített)



Utószó

a biztonság olyan, mint egy lánc:
mértékét mindig a leggyengébb láncszem erőssége határozza meg !