Kriptográfia

Második előadás
Klasszikus titkosítások

Németh L. Zoltán
SZTE, Számítástudomány Alapjai Tanszék
2008 ősz

Szimmetrikus titkosítás (Symmetric Encryption)

- más néven: hagyományos / egy kulcsú
- a feladó és a címzett egy közös titkos kulcson osztozik
- minden klasszikus titkosítás ilyen
- az 1970-es évekig a nyilvános kulcsú kriptográfia megjelenéséig
- ma is a legelterjedtebb, a nyilvános kulcsú módszerek nem lecserélték, hanem kiegészítették őket

Titkosítási alapfogalmak I

- **nyílt szöveg** (paintext): az eredeti érthető üzenet
- **titkosított szöveg** (ciphertext): a titkosítással átalakított üzenet
- **kulcs** (key) a titkosításhoz/megfejtéshez használt kritikus információ.

  (A szimmetrikus kulcsú titkosítás biztonsága azon alapszik, hogy a kulcsot csak a feladó és a címzett ismeri).

Titkosítási alapfogalmak II

- **titkosítás** (enciphering, encryption): a nyílt szöveg "olvashatatlanná tétele" a kulcs segítségével.

  titkosító algoritmus (cipher)

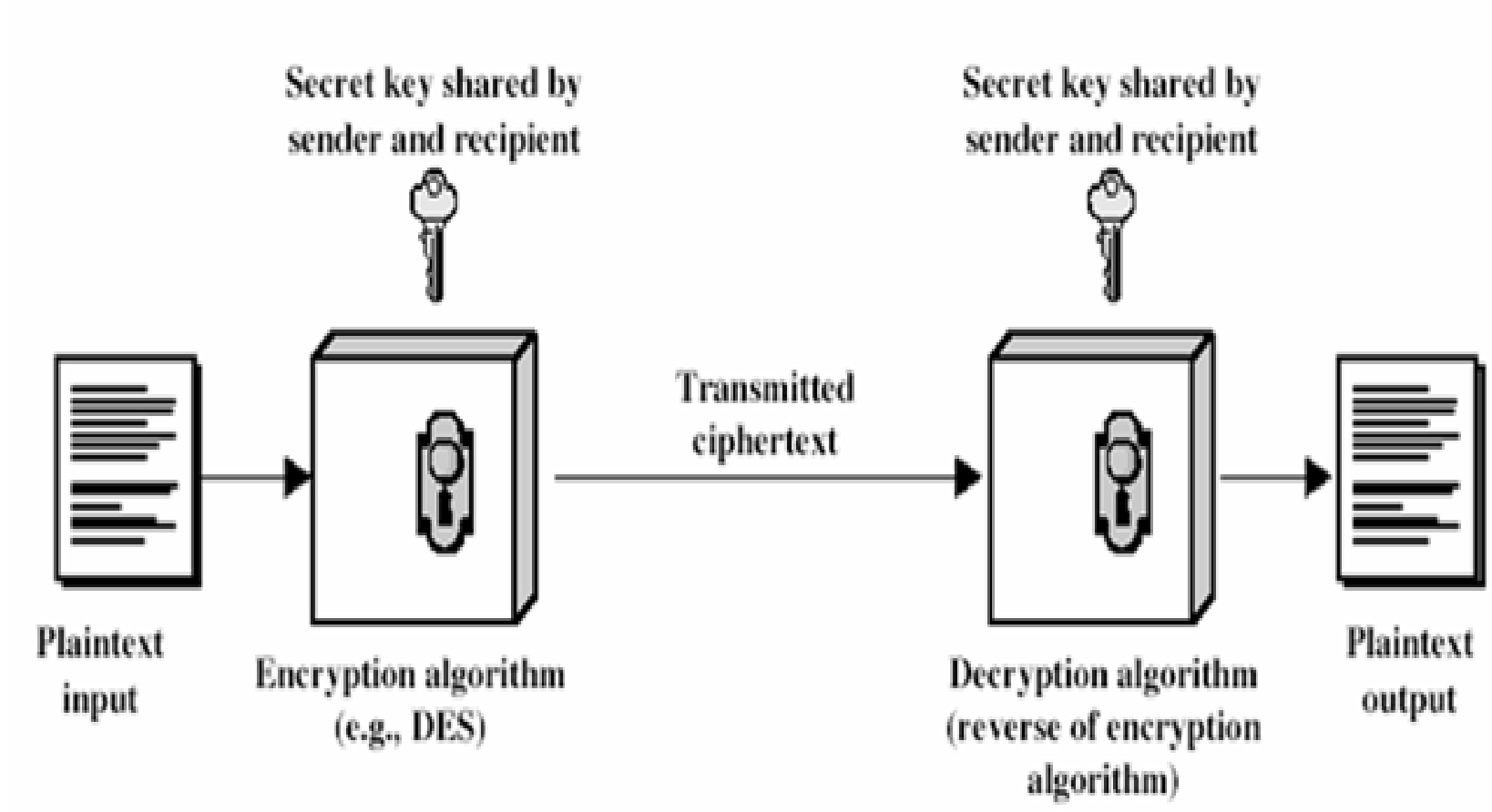
- **megfejtés** (deciphering, description): a títkosított szöveg visszaalakítása nyílt szöveggé a kulcs segítségével.

- **feltörés** (break): /első közelítésben/ a titkosított szövegből a nyílt szöveg rekonstruálása a kulcs ismerete nélkül (Részletesen lásd később a támadásfajták ismertetésénél.)

Résztvevők

- A: (Alíz, Alice) címzett (receiver)
- B: (Bob, Béla) feladó (sender)
- C, D : (Carol, Dave)
  további kommunikáló felek
- E: (Éva, Eve) lehallgató (eavesdropper)
  /passív támadó/
- M: (Máté, Malory) aktív támadó (malicious active attacker)

A szimmetrikus titkosítás modellje



Követelmények

- feltesszük, hogy az algoritmus nyilvános (a Kerckhoff-elv miatt)
- a szimmetrikus titkosítás biztonságához elengedhetetlen, hogy a kulcsot csak

  a feladó és a címzett ismerje
- ezért a kulcsot vagy előre egyeztetni kell vagy más titkos/titkosított csatornán kell eljuttatni (ez a kulcselosztás problémája)
- ha több résztvevő esetén, minden párnak külön kulcsra van szüksége

Alapvető típusok

- keverő titkosítók (P-boxok)
  A titkosított szöveg a nyílt szöveg betűinek permutációja.
- helyettesítő titkosítók (S-boxok)
  A nyílt szöveg betűit (esetleg nagyobb blokkjait) egyesével bijektív módon a titkosított szöveg betűivel helyettesítjük.
- produkciós titkosítók
  keverés-helyettesítés (többszörös) egymás utáni alkalmazása

Teljes kipróbálás (Brute Force)

- mindig lehetséges az összes kulcs kipróbálása
- a legalapvetőbb támadás
- a **kulcstér** (összes kulcsok halmaza) méretével arányos
  (ez exponenciálisan nő a kulcs hosszával!)
- feltételezi hogy a nyílt szöveg ismert vagy felismerhető (megkülönböztethető az értelmetlen jelsorozatoktól)

Feltörés teljes kipróbálással

A kulcs méret (bitekben)	A lehetséges kulcsok száma	Időigény, ha a sebesség 1 megfejtés/μs	Időigény, ha a sebesség 10^6 megfejtés/μs
32	$2^{32} = 4.3 \times 10^{9}$	2^{31} μs = 35.8 perc	2.15 μs
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 év	10.01 óra
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} év	5.4×10^{18} év
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} μs = 5.9×10^{36} év	5.9×10^{30} év
26 betű sorrendje (permutációja)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} év	6.4×10^{6} év

Helyettesítő titkosítók

- a nyílt szöveg betűi (jelei, betűcsoportjai) sorra más betűkkel (jelekkel, betűcsoportokkal) helyettesítődnek
- vagy ha bitenként tekintjük a szövegeket, akkor rögzített hosszú (pl. 64 bit) bitcsoportokat ugyanolyan hosszú bitcsoportokra cserélünk (P-dobozok)
- a jelek pozíciója változatlan marad

Caesar titkosító (Caesar Cipher)

- a legkorábbi ismert helyettesítő titkosító
- Julius Caesartól
- az első bizonyítottan használt háborús alkalmazása a kriptográfiának
- helyettesítsünk minden betűt az ábécé rendben utána következő harmadik betűvel
- például:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

- CryptTool bemutató: http://www.cryptool.com/

Eltoló/léptető titkosító (Shift Cipher)

- helyettesítsünk minden betűt az ábécé rendben utána következő k-dik betűvel
- Caesar a k=3 kulcsot használta.
- k=3 –ra a helyettesítés:

```
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
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
```

- a matematikai leíráshoz a betűket számokkal azonosíthatjuk:

```
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
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
```

- a nyílt szöveg betűi kisbetűk,
- a titkosított szövegéi nagybetűk
- a magyar szövegeket is ékezet nélkül tekintjük

Kriptorensdszer (Cryptosystem)

Def. Kriptorendszernek egy $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ ötös, ahol

1. $\mathcal{P}$ a lehetséges nyílt szövegek halmaza
2. $\mathcal{C}$ a lehetséges titkosított szövegek halmaza
3. $\mathcal{K}$ a kulcstér, a lehetséges kulcsok véges halmaza
4. Minden $K \epsilon \mathcal{K}$-ra létezik egy
   $e_K \epsilon\, \mathcal{E}$, $e_K : \mathcal{P} \rightarrow \mathcal{C}$ egy titkosító leképezés,
   $d_K \epsilon\, \mathcal{D}$, $d_K : \mathcal{C} \rightarrow \mathcal{P}$ egy megfejtő leképezés, hogy
   $d_K(e_K(x)) = x$ teljesül minden $x \epsilon\, \mathcal{P}$-re.

Vegyük észre, hogy e_K injektív fgv. kell hogy legyen.

Az eltoló kriptorendszer

$\mathcal{P}=\mathcal{C}=\mathcal{K}=\mathbf{Z_{26}}$ és minden $0 \le K \le 25$ -re

$$e_K(x) = (x + K) \bmod 26,$$

és

$$d_K(x) = (x - K) \bmod 26$$

$(x,y \in \mathbf{Z_{26}})$

Kriptoanalízise

- csak 26 lehetséges kulcs van:
  - „a” képe lehet A,B,…,Z
- ezek sorra kipróbálhatók
- azaz teljes kipróbálással feltörhető
- csak kódszöveg típusú támadással
- persze ehhez fel kell tudni ismerni a nyílt szöveget
- pl. törjük fel: "GCUA VQ DTGCM"

Egyábécés helyettesítés (Monoalphabetic Substitution)

- az ábécé betűinek egyszerű letolása helyett
- tetszőlegesen össze is keverhetjük a betűket
- így minden nyílt betűt egy titkossal helyettesítünk
- különböző nyílt betűket különbözőekkel
- ekkor e kulcs a 26 betű egy sorrendje

```
KULCS:  abcdefghijklmnopqrstuvwxyz
        DKVQFIBJWPESCXHTMYAUOLRGZN

nyílt szöveg : ifwewishtoreplaceletters
titkos szöveg: WIRFRWAJUHYFTSDVFSFUUFYA
```

Egyábécés helyettesítő kriptorendszer

$\mathcal{P}=\mathcal{C}=\mathbf{Z_{26}}$,

$\mathcal{K}$: a 0,1, ..., 25 számok összes lehetséges permutációja

Minden π: $\mathbf{Z_{26}} \rightarrow \mathbf{Z_{26}}$ $\epsilon\mathcal{K}$ permutációra

$$e_{\pi}(x) = \pi\ (\ x\ )\ ,$$

és

$$d_{\pi}(x) = \pi^{-1}\ (\ x\ )$$

$$(\ \ x,y\ \epsilon\ \mathbf{Z_{26}}\ )$$

Ahol π^{-1} a π inverz permutácuiója.

Spec.esete: az affin titkosító

$\mathcal{P}=\mathcal{C}=\mathbf{Z}_{26}$,
$\mathcal{K}$:= { (a,b) ϵ | $\mathbf{Z}_{26}$ **x** $\mathbf{Z}_{26}$ lnko(a,b) = 1 }
Minden K = (a,b) ϵ $\mathcal{K}$-ra legyen

$$e_K(x) = (ax + b) \bmod 26 ,$$

és

$$e_K(y) = a^{-1}(y - b) \bmod 26$$

(x,y ϵ $\mathbf{Z}_{26}$)

Ahol a^{-1} az *a* multiplikatív inverze a $\mathbf{Z}_{26}$-ban, azaz
$a\ a^{-1} \equiv 1 \pmod{26}$.
Részletesebben gyakorlaton.

Az egyábécés helyettesítés kriptoanalízise

- a kulcstér most $26! \approx 4 \times 10^{26} \approx 2^{88.4}$ elemű
- ez biztonságosnak látszik
- de ez csak a teljes kipróbálás ellen véd
- NEM BIZTONSÁGOS !!!
- a kriptoanalízis a nyílt szöveg nyelvének nyelv statisztikai sajátosságain alapszik
- gyakorlatban egy legalább 50 betűs szöveg megfejthető

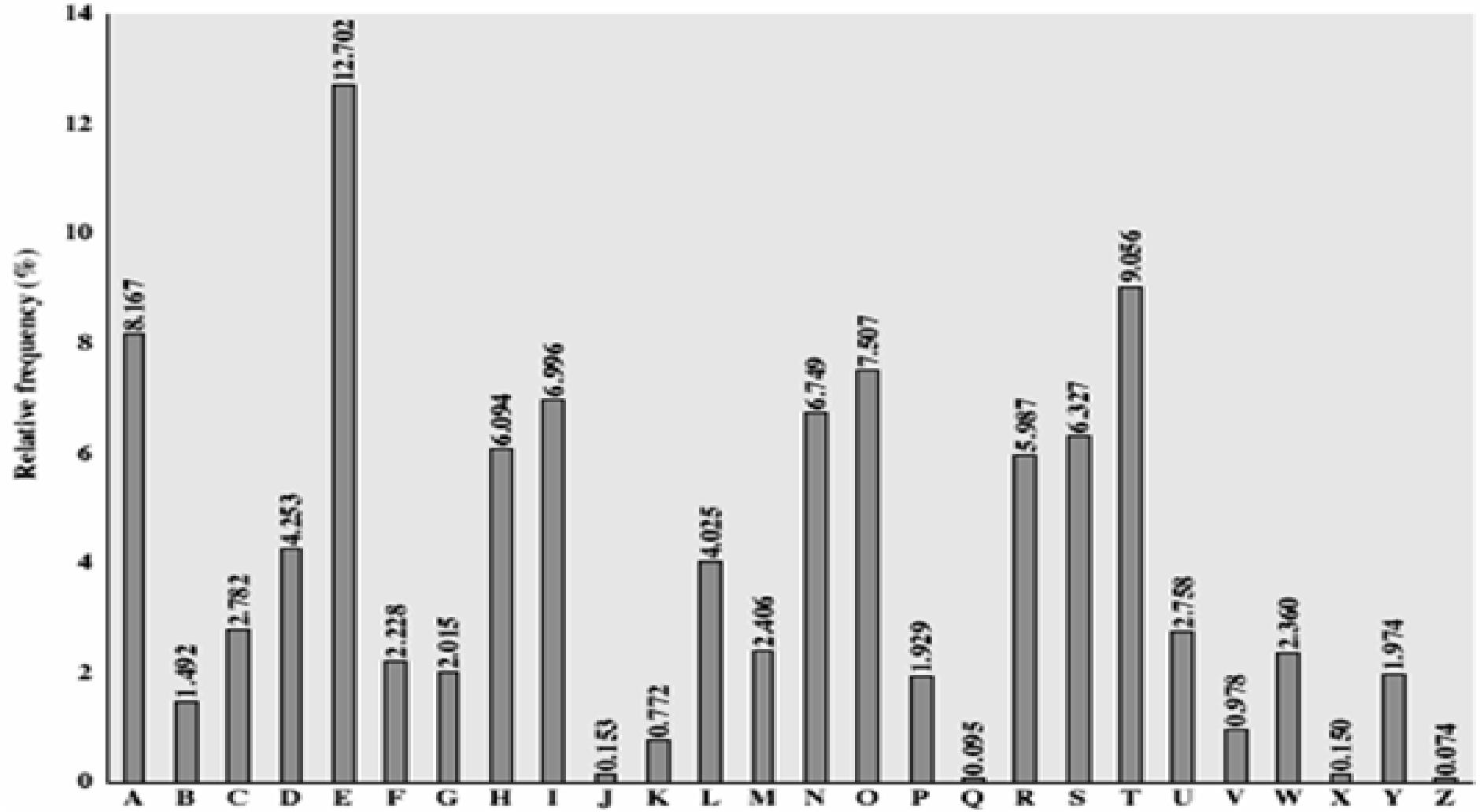
Nyelvi statisztikák I

- az emberi nyelvek **redundánsak**
- pl. a magánhangzók elhagyhatók:
  "bc bc trk s fl s frk"
- nem minden betű egyformán gyakori
- az angolban: E, T,A,O,I,N,S,H,R....,J,X,Q,Z
- magyarban (ékezetekkel)
  - a leggyakoribb az "E", "A" és "T"
  - majd "L", "N", "S", "K", "O", "R"
  - igen ritka: "Ő", "W", "X", "Q"

Nyelvi statisztikák II

- hasonlóan lehet a betűpárok (digram), hármasok (trigram) gyakoriságát vizsgálni pl. ”SZ”, ”TT”, "THE"
- ezek a statisztikák a nyelvekre jellemzőek segítségükkel a nyílt szöveg nyelve azonosítható
- MÁS MÓDSZER: gyakori / jellemző szavak keresése: pl. pénzügyi szövegben millió = ABBA minta, időjárásjelentésben: eső

Betűgyakoriságok az angolban



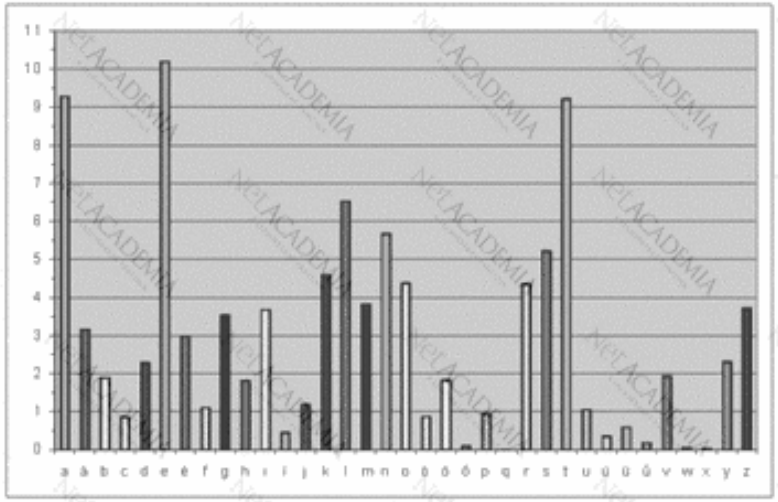
Betűgyakoriság a magyarban

q	0,003
x	0,027
w	0,047
ő	0,092
ü	0,177
ú	0,343
í	0,439
ü	0,589
c	0,849

ó	0,871
p	0,934
u	1,043
f	1,098
j	1,179
h	1,808
ö	1,830
b	1,887
v	1,922

d	2,284
y	2,305
é	2,979
á	3,159
g	3,527
i	3,667
z	3,721
m	3,819
r	4,346

o	4,364
k	4,586
s	5,212
n	5,671
l	6,523
t	9,213
a	9,278
e	10,189



58. ábra ABC rendes betűgyakoriság magyar szövegben

Használatuk a kriptoanalaízisben

- az egyábécés helyettesítés nem változtatja meg a betűgyakoriságot
- már az arabok is felfedezték a IX. században
- számoljuk ki a titkosított szöveg betűinek/betűpárjainak gyakoriságát
- tippeljünk az ismert statisztika és/vagy a gyakori szavak alapján a betűk képeire
- ha valószínűleg értelmetlen szövegrészt kapunk, pl: "EE" akkor módosítsunk a tippünkön
- az értelmes szótöredékek/szavak újabb tippekre adnak lehetőséget
- folytassuk, amíg a szöveget meg nem fejtjük

Egy angol példa

- given ciphertext:

  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
  VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
  EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- számoljuk ki a betűgyakoriságot
- tipp: P és Z megfelel e –nek és t-nek
- tipp: ZW = th (ez a leggyakoribb digram)
  így ZWP = the
- további próbálkozások és javítások után:

  it was disclosed yesterday that several informal but
  direct contacts have been made with political
  representatives of the viet cong in moscow

Kriptogrammok

- Ha a szóközöket és az írásjeleket meghagyjuk, sokkal könnyebb az egyábécés helyettesítés feltörése, rövid titkosított szöveg esetén is.
- Az ilyen rejtvényeket hívják kriptogrammoknak.
- Néha egy-egy betűt segítségül előre megadnak.
- Külön statisztika készíthető a szókezdő/szózáró betűkről
- Lásd részletesebben: http://hu.wikipedia.org/wiki/Kriptogram
- Angol online kriptogrammok és nyelvi statisztikák: http://www.cryptograms.org/

A helyettesítés változatai

- Mint láttuk az egyábécés helyettesítés könnyen feltörhető, mert a kódszöveg megtartja a nyílt szöveg betűgyakoriságait.
- Ezen több módon lehet javítani, nehezebbé (de nem lehetetlenné!) téve a kriptoanalízist:
  1. homofónok használata
  2. nagyobb egységek pl. betűpárok helyettesítése pl. ilyen a Playfair titkosító
  3. több ábécés helyettesítések pl. Enigma

1. Homofónok használata

- egy betűt több jellel is helyettesíthetünk
- a gyakoribb betűknek több képük van
- ezzel "elrejthetjük" ugyan betűgyakoriságokat
- de a több-betűs minták gyakorisága továbbra is megmarad
- egyenes utat adva ezzel a kriptoanalízisnek
- pedig C. F. Gauss feltörhetetlennek gondolta
- Ld. Cryptools: Homophones

2. A Playfair titkosító

- betűpárok betűpárokkal való helyettesítésén alapul
- Charles Wheatstone találta fel 1854-ben, de a barátjáról Baron Playfairről nevezte el
- az angol hadsereg széles körben használta az I. világháborúban
- de még előfordult a II-ban is.
- előnye, hogy egy személy eszköz segítsége nélkül papíron használhatja

Playfair kulcsmátrix

- egy 5X5-ös mátrix melynek első betűit a kulcsszó határozza meg
- a kulcsszó betűinek csak az első előfordulását vesszük
- a mátrix többi részét kitöltjük a maradék betűkkel Pl. ha a kulcsszó MONARCHY:

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

Titkosítás és megfejtés

A nyílt szöveg betű párokra osztjuk, ha egy kódolandó pár egy betű ismétlése, akkor egy elválasztó betűt, mondjuk 'X'-et teszünk közéjük és ezután kódoljuk.
Pl. balloon -> ba lx lo on

1. ha a két betű egy sorban van, helyettesítsük őket a tőlük közvetlenül jobbra lévő betűkkel (a sor vége után a sor első betűjére ugorva) Pl. ar -> RM

2. ha a két betű egy oszlopban van, helyettesítsük őket a tőlük közvetlenül alattuk lévő betűkkel (az oszlop alja után az legfelső betűre ugorva) Pl. mu -> CM

3. különben a betűk kódja a saját sora és a másik betű oszlopának metszetében álló betű. Pl. hs -> BP, ea -> IM

A Playfair titkosító biztonsága

- jóval erősebb az egyábécés helyettesítésnél
- mivel 26 x 26 = 676 betűpár van
- a gyakoriság táblázathoz így 676 gyakoriságérték kell (szemben a 26 betűvel)
- így hosszabb titkos szövegre van szükségünk
- de fel lehet törni néhány száz betűs szöveg esetén is
- mivel a nyílt szöveg struktúrájából még mindig sok tükröződik a titkosított szövegben

3. Többábécés titkosítók (Polyalphabetic Ciphers)

Két közös jellemzőjük:

1. betűnként más-más (egymással összefüggő) ábécét, pontosabban egyábécés helyettesítést használnak
2. hogy mikor melyik ábécé kerül sorra, a kulcs határozza meg

- általában a kulcs véget érése után a használt ábécék ciklikusan ismétlődnek
- minél több az ábécé, annál jobban kiegyenlítődik a betűgyakoriság
- megnehezítve ezzel a kriptoanalízist

A Vigenère titkosító

- a legegyszerűbb, és legismertebb többábécés helyettesítés
- ábécéként eltoló (shift) titkosítókat használ
- a kulcs egy *d* betűs szó $K = k_1\ k_2\ ...\ k_d$
- a nyílt szöveg *i*-dik betűjét a kulcs az *i*-dik betűjével azaz k_i-vel toljuk el
- a *d*-dik betű titkosítása után a kulcs és így az eltolások ciklikusan ismétlődnek
- a megfejtés ugyanez, csak fordított irányú eltolásokkal

Példa Vigenère titkosításra

- írjuk le a nyílt szöveget
- írjuk fölé a kulcsszót ciklikusan ismételve
- alkalmazzuk minden betűre a felette levő betűvel való eltolást
- pl. ha a kulcsszó *deceptive*

```
kulcs:        deceptivedeceptivedeceptive
nyíltszöveg: wearediscoveredsaveyourself
titkosított: ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

- CryptTool bemutató: http://www.cryptool.com/

A Vigenére titkosító

Legyen d pozitív egész. $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbf{Z_{26}})^d$

Minden $K = (k_1, k_2, \ldots, k_d) \in \mathcal{K}$-ra legyen

$$e_K(x_1, x_2, \ldots, x_d) = (x_1 + k_1, x_2 + k_2, \ldots, x_d + k_d),$$

és

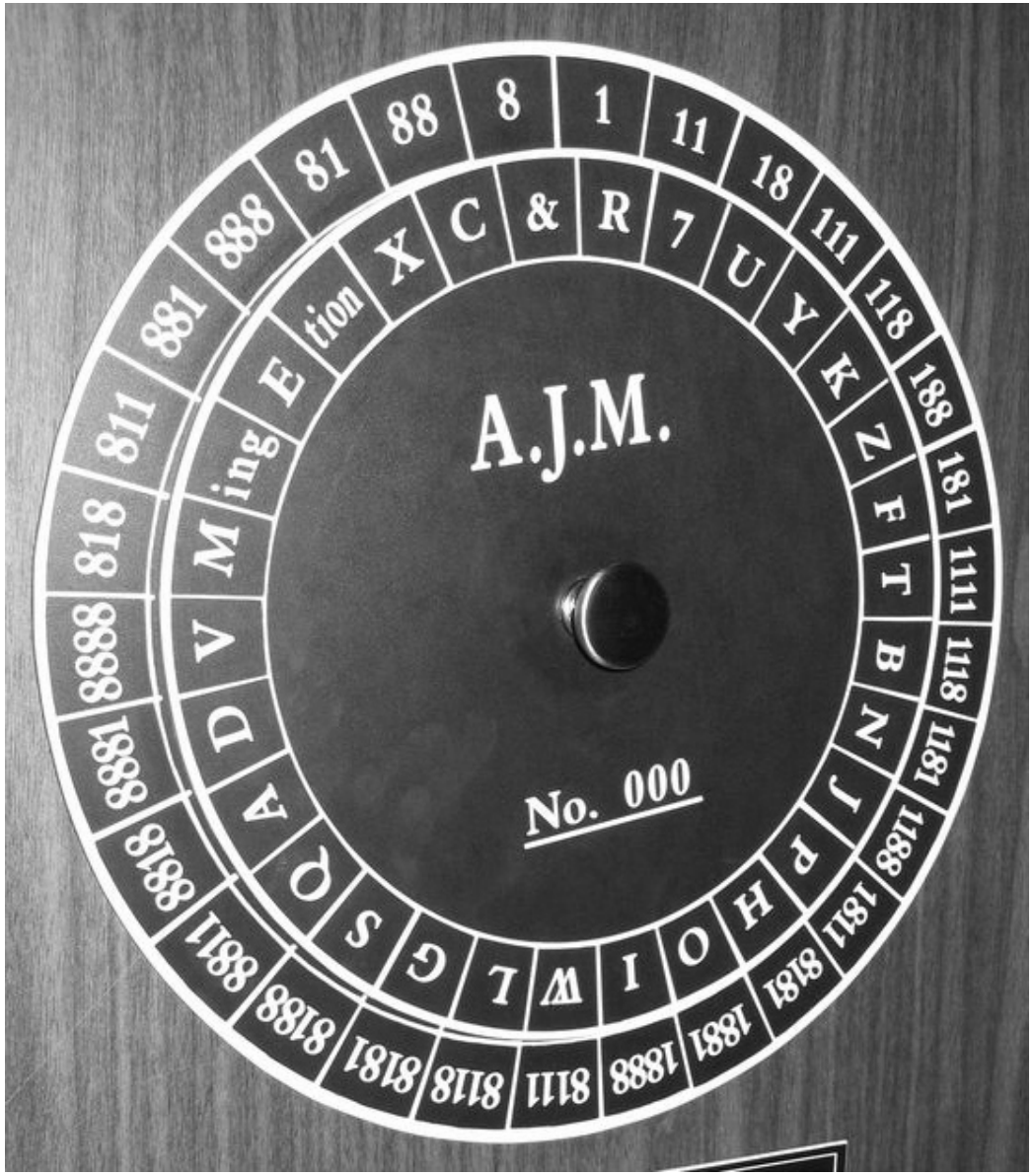
$$d_K(y_1, y_2, \ldots, y_d) = (y_1 - k_1, y_2 - k_2, \ldots, y_d - k_d),$$

Ahol a műveletek mindenhol $\mathbf{Z_{26}}$-ban végzendők.

Segédeszközök

- **Saint-Cyr szalag** egyszerű manuális segítség
  - két egymáson elcsúsztatható léc az ábécé két-két példányával
  - a felső 'a' betű alá mozgatva az 'a' nyílt betű képének alsó lécen található első példányát
  - minden betű eltoltja egyszerűen leolvasható
- a szalagot összehajtva egy **titkosító lemezhez** jutunk
- vagy kiírhatjuk egy táblázatba az összes eltolást, így kapjuka **Vigenère-tablót**

Titkosító lemez (az amerikai polgárháborúból)



http://en.wikipedia.org/wiki/Cipher_disk

Vigenère-tabló

	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

http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

A Vigenère-titkosító kriptoanalízise

- egy nyílt betűt több titkos betű helyettesíthet, attól függően, hogy melyik kulcsbetű alá esik
- ez összezavarja a betűgyakoriságokat
- de nem rejti el teljesen

Két feladat van:

- a kulcs hosszának, azaz az ábécék számának meghatározása
- ezek után az azonos kulcsbetűvel titkosított betűkre külön-külön az eltolások mértékének meghatározása

A Kasiski-teszt

- Babbage / Kasiski által kifejlesztett módszer
- a titkosított szöveg ismétlődései származhatnak azonos nyílt szöveg részekből, ha távolságuk a kulcshossz többszöröse
- ezért keressük meg a titkosított szöveg legalább 3 betűs ismétlődéseit, és határozzuk meg a távolságukat
- persze előfordulhat, hogy az egybeesés véletlen, és nem azonos nyílt szövegekből származik
- de a kulcshossznak a véletlen kivételektől eltekintve a távolságok mindegyikét osztania kell
- pl. a példában a két "VTW" távolsága 9
- ami azt sugallja, hogy a kulcshossz 3 vagy 9

Egybeesés-számlálás

- William F. Friedman talált fel (1920 körül)
- Nyelvi szövegben nagyobb a valószínűsége, hogy két véletlenül választott pozíción ugyanaz a betű szerepel, mint véletlen betűkből álló szövegben.
- Pl. angolban ≈ 6.5%,
- véletlen szövegben ≈ 3.8%
- ez lehetőséget biztosít a kulcshossz és az eltolás mértékének meghatározására is
- Ld. CryptTool automatikus Vigenère analízis

Vigenère autokulcsos titkosító (Vigenère autokey Cipher)

- Akkor ideális a többábécés helyettesítés, ha a kulcs ugyanolyan hosszú, mint a nyílt szöveg
- Vigenère javasolta az autokulcsos titkosítót változatát a Vigenère-titkosítónak
- a kulcs vége után a nyílt szöveg elejét használjuk „kulcsként” folytatólagosan
- Pl. ha a kucs továbbra is *deceptive*

```
key:        deceptivewearediscoveredsav
plaintext: wearediscoveredsaveyourself
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
```

Kriptoanalízise

- Úgy tűnik ezzel kiküszöböltük a Vigenére-titkosítás gyenge pontját a periodikus ismétlődéest
- De sajnos közben a titkosított szöveg még közvetlenebbül függ a nyílt szövegtől
- Pl. minden megfejtett vagy csak megsejtett nyílt szöveg rész újabb nyílt szöveg részt fejt meg
- A gyakori betűk egybeesések gyakorisága miatt ‘E’ legtöbbször ‘E’-vel lesz titkosítva
- Így valójában gyengébb titkosításhoz jutunk mint az eredeti Vigenére-titkosítás

Tanúság

- Házi feladat:

  Még könnyebben feltörhető rendszert kapunk ha a kulcs után a kódszöveg és nem a nyílt szöveg betűit használjuk további kulcsokként.
- A titkosító rendszer bonyolítása nem feltétlenül vezet a biztonság növeléséhez.
- Sőt, a megbízható titkosítások néha igen egyszerűek.

Vernam-titkosító

- Ideális estben a kulcs ugyanolyan hosszú, mint a nyílt szöveg
- Ezt Gilbert Vernam (AT&T) javasolta 1918-ban
- Az ő rendszere bitenként dolgozik:

$$c_i = p_i \text{ XOR } k_i$$

- Ahol p_i = a nyílt szöveg i-dik bitje

k_i = a kulcs i-dik bitje

c_i = a titkosított szöveg i-dik bitje

XOR = a kizáró vagy művelet,

0 XOR 1 = 1 XOR 0 = 1

0 XOR 0 = 1 XOR 1 = 0

A XOR művelet kedvező tulajdonságai

- XOR = „kizáró vagy” (1 XOR 1 = 0 miatt)
- Jeölni szokták még így: $\oplus$
- Tulajdonségai:

  x XOR y = y XOR x

  x XOR (y XOR z) = (x XOR y) XOR z

  x XOR x = 0

  x XOR 0 = x
- Ezért (x XOR y) XOR y = x, vagyis ha kétszer végezzük el a XOR-olást ugyanazzal az y-nal, visszakapjuk az eredeti x-et.

A megfejtés és a titkosítás algoritmusa megegyezeik.

Példa

Nyílt szöveg:	**00**	**10**	**11**	**01**	**10**
Kulcs:	10	11	01	10	11
Titk. szöveg:	**10**	**01**	**10**	**11**	**01**
Kulcs:	10	11	01	10	11
Nyílt szöveg:	**00**	**10**	**11**	**01**	**10**

Egyszeri hozzáadásos titkosító I (one-time pad)

- ha a kulcs valóban véletlen és ugyanolyan hosszú, mint a nyílt szöveg a titkosító nem törhető fel (=feltétlenül biztonságos)
- Ezt a két feltétel azonban szigorúan be kell tartani, például nem szabad ugyanazzal a kulccsal még egyszer üzenetet titkosítani (innen az egyszeri név)
- Ezt hívják egyszeri hozzáadásos módszernek One-Time pad: OTP
- A OTP azért feltörhetelen mert a titkosított szövegnek nincs statisztikai kapcsolata a nyílt szöveggel

Egyszeri hozzáadásos titkosító II

- mivel minden nyílt-titkos szövegpárhoz létezeik (pontosan) egy kulcs amivel titkosíthattuk
- ha kulcsot valóban véletlenszerűen választottuk
- nincs rá mód, hogy kitaláljuk melyik kulcs az igazi, hiszen minden elképzelhető értelmes nyíltszöveghez van egy kulcsunk.

- a gyakorlatban két nehéz probléma van vele:
  - valóban véletlen kulcsgenerálás
  - a kulcselosztás és tárolás problémája

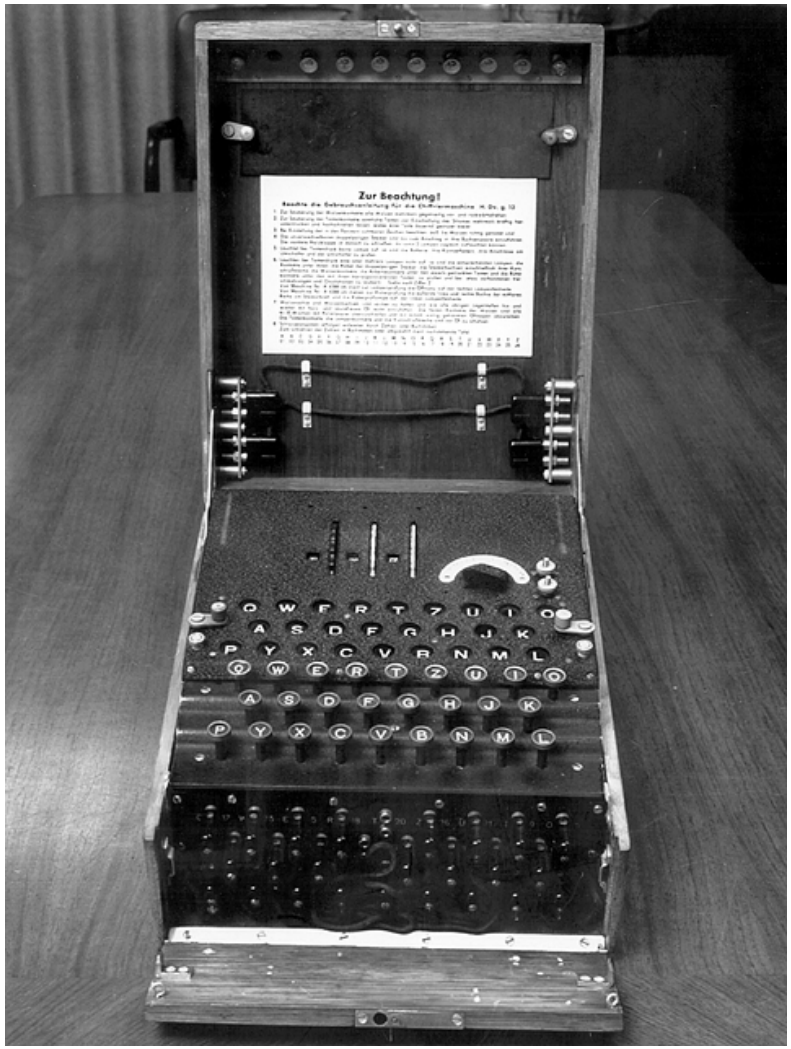
Alkalmazása

- Ezek a gyakorlati problémák alkalmazását erősen korlátozzák.
- Csak alacsony sávszélesség és nagyon nagy biztonsági igény esetén
- Pl. Amerikai – szovjet diplomácia
- Kémek tájékoztatása:
  Numbers Station-ök
  (számokat sugárzó rádióadók)
- Ld: http://en.wikipedia.org/wiki/Numbers_station

Rotoros gépek (Rotor Machines)

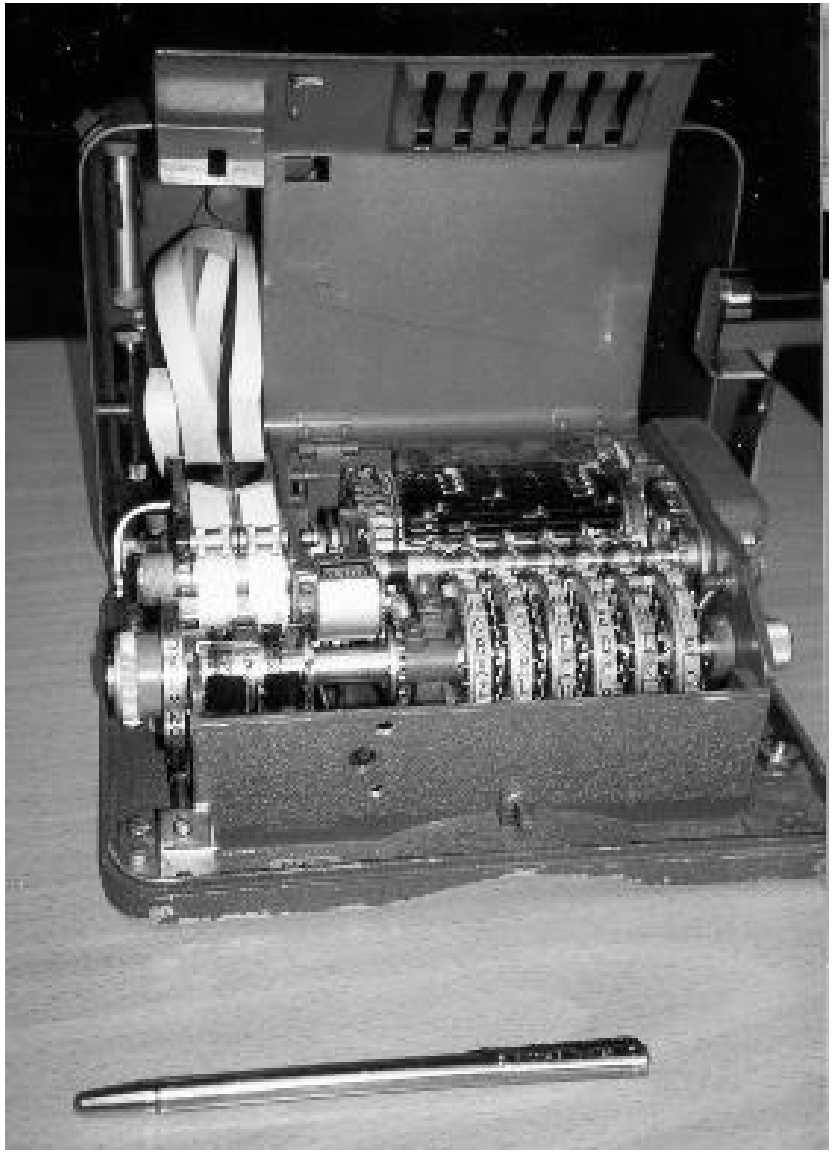
- a számítógépek és ezzel a modern titkosítók megjelenése előtt a rotoros gépek voltak a legelterjedtebb komplex titkosító eszközök
- Széles körben használták a II. világháborúban:
  - németek: Enigma, szövettségesek: Hagelin, japánok: Purple
- Igen bonyolult többábécés helyettesítések
- forgó korongok (rotorok) segítségével, melyek egy-egy egyszerű helyettesítést kódoltak, de minden betű titkosítása után **számlálószerűen különböző sebességgel forogtak**
- pl. egy 3 rotoros gép 26^3=17576 ábécével dolgozott
  Működés: http://enigmaco.de/index-enigma.html

Az Enigma



http://en.wikipedia.org/wiki/Enigma_machine

A Hagelin



Enigma szimulátorok

- http://frode.home.cern.ch/frode/crypto/simula/index.html

  Közülük két ajánlott példány:
- http://users.telenet.be/d.rijmenants/
- http://www.xat.nl/enigma/

Az Enigma felépítése, működése, kódkönyvek, kódolás, dekódolás bemutatása a Rijmenants szimulátorával

Keverő titkosítók
Transposition Ciphers

- a helyettesítés mellett a másik alap titkosítási módszer a keverés (pemutációk)
- a szöveg egységek (betűk/bájtok/bitek/bitcsoportok) megmaradnak
- csak a sorrendjük változik meg
- alkalmazásuk felismerhető, mert a jelekgyakoriságát nem változtatják meg.

Skitlai (scytale)

- Spártaiak használták
- katonai célokra
- a kulcs a bot átmérője

Kerítés rács elrendezés (Rail Fence cipher)

- írjuk le az üzenetet átlósan lefelé több sorba
- majd olvassuk el soronként balról jobbra haladva
- pl. (csak két sort használva)

```
m e m a t r h t g p r y
  e t e f e t e o a a t
```

- a titkosított szöveg:

```
MEMATRHTGPRYETEFETEOAAT
```

Soronként cserélő titkosítók (Row Transposition Ciphers)

- bonyolultabb keverést kapunk, ha
- az üzenetet soronként adott számú oszlopba írjuk
- majd az oszlopokat a kulcs által megadott sorrendben olvassuk össze felülről lefelé
- Kulcs: 3 4 2 1 7 5 6

```
Nyílt szöveg:   a t t a c k p
                o s t p o n e
                d u n t i l t
                w o a m x y z
 Titk. szöveg: TTNAAPTMTSUOAODWPETZCOIXKNLY
```

Duplán keverő titkosító

Még biztonságosabb titkosításhoz jutunk, ha

- Ha az előző keverést kétszer végezzük el, különböző kulcsokkal (azaz permutációkkal)
- A kulcsok által meghatározott premutációja az oszlopoknak különböző elemszámú
- véletlen betűkkel töltjük ki az üzenet végét, hogy teljes sorokat kapjunk

A permutációkat jelszavak segítségével is elő lehet állítani. Ld.

- Cryptool Permutation/Transposition Cipher
- Duplán keverő titkosítás (gyakorlat)

Produkciós titkosítók (Product Ciphers)

- sem a helyettesítő, sem a keverő titkosítók nem biztonságokat, a nyelv jellegzetességei miatt
- ötlet:alkalmazzuk őket egymás után, hogy erősebb titkosításhoz jussunk, de:
  - két helyettesítés eredménye egy újabb (általában komplexebb) helyettesítés
  - két keverés egymásutánja továbbra is egy újabb keverés
  - de ha a keveréseket és a helyettesítéseket egymás után váltogatjuk (esetleg többször) valóban erősebb titkosításhoz jutunk
- a különböző elvű titkosítások keverése vezet a modern szimmetrikus módszerekhez

Titkosítók generációi

- Első generáció: XVI-XVII. századig, főleg egyábécés helyettesítések (pl. Caesar)
- Második generáció: XVI-XIX században, többábécés helyettesítések (pl. Vigenére)
- Harmadik generáció: XX sz. elejétől Mechanikus és elektromechanikus eszközök (pl. Enigma, Hagelin, Putple, Sigaba)
- Negyedik generáció: a XX. század második felétől produkciós titkosítók, számítógépekkel (pl. DES, Triple DES, Idea, AES)
- Ötödik gemneráció: kvantumelvű titkosítások, sikeres kisérletek vannak rá, de gyakorlati alkalmazásuk ma még futurisztikus ötletnek tűnhet

Felhasznált irodalom

- Virrasztó Tamás: Titkosítás és adatrejtés: Biztonságos kommunikáció és algoritmikus adatvédelem, NetAcademia Kft., Budapest, 2004. Online elérhető: http://www.netacademia.net/book.aspx?id=1#
  (2. fejezet)
- William Stallings: Cryptography and Network Security, 4th Edition, Prentice Hall, 2006. (Chapter 2)
- Lawrie Brown előadás fóliái (Chapter 2)
- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone : Handbook of Applied Cryptography, CRC Press, 1996, online elérhető: http://www.cacr.math.uwaterloo.ca/hac/ (Chapter 1)
- D. R. Stinson: Cryptography, Theory and Practice, Chapman & Hall/CRC, 2002
  (Chapter 1)