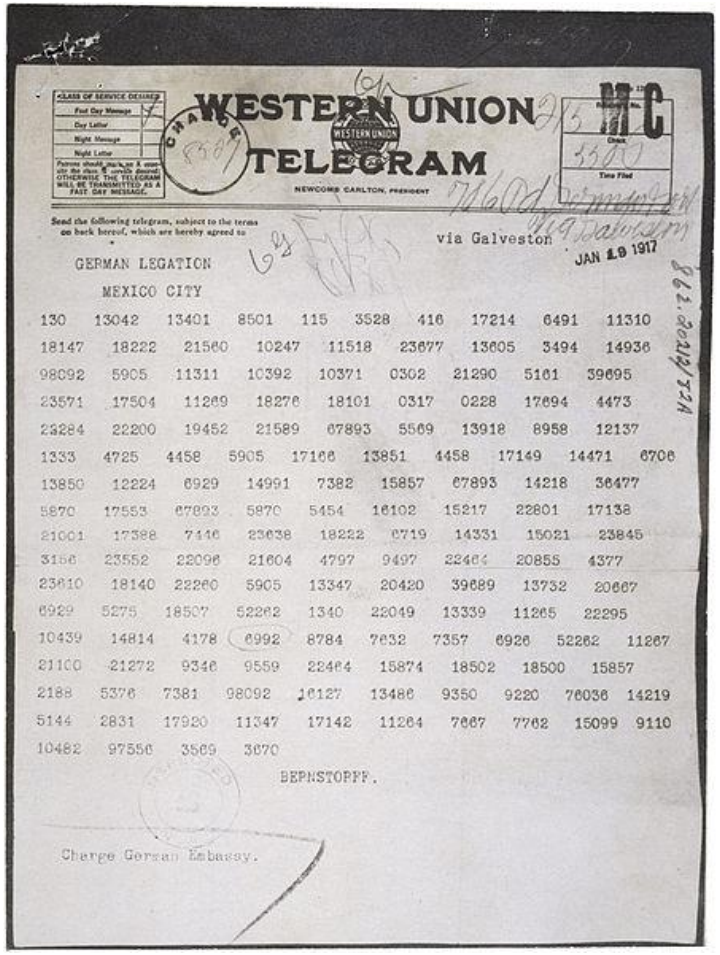
Kriptográfia

BME - TMIT
VITMA378 - Médiabiztonság
feher.gabor@tmit.bme.hu

Titkosítás / Cryptography

- Cryptography
  - Görög szó: titok írás
    - A titkosítás látható, de az üzenet ismeretlen
- Alap jelölések
  - Nyílt szöveg / Plaintext (P)
  - Titkosított szöveg / Ciphertext (C)
  - Kulcs / Key (K)
  - Titkosítás: $C = E_K(P)$
  - Titkosítás feloldása: $P = D_K(C)$



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

Titkosítás feltörése / Cryptanalysis

- Titkosított szöveg felfedése kulcs ismerete nélkül
- Titkosított szöveg módosítása kulcs ismerete nélkül

- Kulcs megszerzése
  - Ismert nyílt szöveges támadás
    - A szöveg egyes részlete (P_1) és titkosított formája (C_1) ismert a támadó részéről
    - Pl.: ZIP archívumok ismert fájlokkal
  - Side channel attack
    - A titkosító rendszer implementációjában mérhető információkat is felhasználjuk a töréshez
    - Pl.: RSA törések

Titkosítás feltörése (folyt.)

- Kulcs megszerzése (folyt.)
  - Hiba a titkosító algoritmusban
    - Speciális plaintext és az erre generált ciphertextből megismerhető a kulcs
    - Hibás algoritmusok
    - Pl.: RC4 problémák
  - Kulcsok próbálgatása
    - Nyers erő – szótár - okos erő támadások
      - Brute force: Minden kulcsot tesztelek
      - Dictionary: Csak egy megadott kulcskészletet tesztelek
      - Smart force: Minden kulcsot tesztelek, de valószínűségük sorrendjében
    - Szivárvány táblák
      - Törési sebesség növelése előredolgozással

Security, obscurity, design

- Security by obscurity
  - A titkosító eljárás ismeretlen és a feltalálók úgy gondolják, hogy lehetetlen megfejteni azt
  - Elemzés hiányában rejtett hibákat tartalmazhat
  - Súlyos problémák lehetnek, ha az eljárást megfejtik/ellopják

- Security by design
  - A titkosító algoritmus/eljárás publikus. A titkosságot a felhasználás során a kulcs biztosítja
  - Kriptológusok elemezhetik az eljárást, hibákat keresnek
  - A kevesebb titok erősebb rendszert eredményezhet

- Kerckhoffs' principle (XIX. sz.) és Shannon's maxim (XX. sz.)
  - „A kulcson kívül minden ismert” - „Az ellenség mindent ismer”

A kriptográfia története
Klasszikus titkosítás

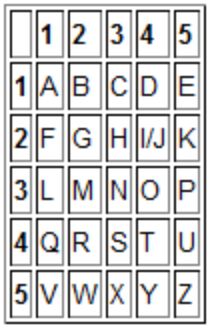
- ~ 2500 BC
  - Hagyományostól eltérő hieroglifák egyiptomi sírokon. Nem titkot fejez ki, hanem inkább a fontosságot, varázslatot jelöl. Titok és misztikum.

- ~ 600 BC
  - Egyszerű, egyábécés (monoalphabetic) helyettesítő titkosítások
    - Atbash titkosító: héber helyettesítő titkosító (Az ABC megfordítás)
      - ABCDEFGHIJKLMNOPQRSTUVWXYZ
      - ZYXWVUTSRQPONMLKJIHGFEDCBA

- ~400 BC
  - *Görögök: Szteganográfia megjelenése*
    - Hérodotosz írása leborotvált fejű rabszolgákról, agyagtáblák
  - Titkosítás eltolással (~700 BC ?)
    - A spártai hadsereg titkosítása: Scytale
      - Papiruszt tekernek egy bot köré és erre írják az üzenetet a bot irányában. Megfejtés egy ugyanolyan átmérőjű bottal

Klasszikus titkosítás (folyt.)

- ~ 200 BC
  - Polybius (görög) négyzet. Az ABC-t egy 5x5 –ös négyzetbe írta, és a pozíciót jelölő számokat használta betűk jelölésére
  - Jelzés a távolba (publikus csatorna)



	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

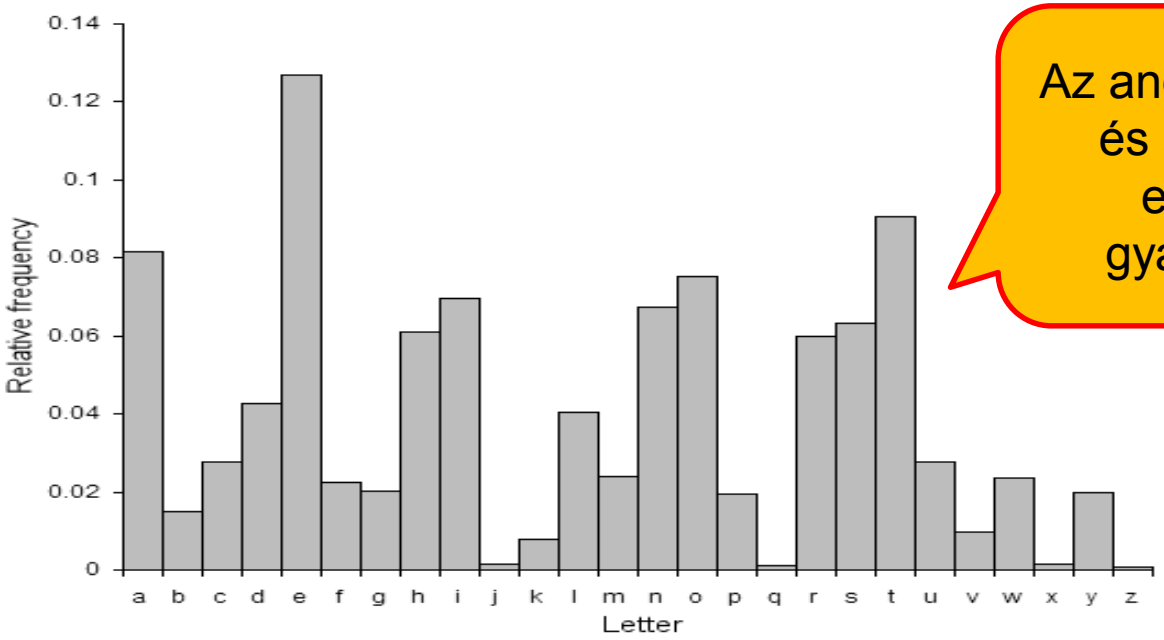
- ~ 50 BC
  - Római: Ceasar titkosító. A betűk eltolása 3 pozícióval
    - ABCDEFGHIJKLMNOPQRSTUVWXYZ
    - DEFGHIJKLMNOPQRSTUVWXYZABC
- ~ 400 AD
  - *India: Titkos kommunikáció (Kama sutra)*

A kriptográfia története
Középkori titkosítás

- ~ 800
  - Al-Kindi (irak): Az egyábécés titkosítások feltörése frekvencia analízissel. Ezzel egy időben utal a többábécés (polyalphabetic) titkosításra is.
- ~ 1350
  - Taj ad-Din Ali ibn ad-Duraihim ben Muhammad ath-Tha 'alibi al-Mausili (Egyiptom): titkosítás többszörös helyettesítéssel (csak utalás, a mű elveszett)
- 1466
  - Leon Battista Alberti (Olasz művész és tudós): A többábécés titkosítás „feltalálója”
    - Father of Western Cryptology

Gyakoriság vizsgálat
Frekvencia analízis

- A betűk sűrűségfüggvénye jellemző
  - A helyettesítéshez használt kulcs megfejthető



Az angol ABC betűi és a nyelvben előforduló gyakoriságuk

Többábécés titkosítás

- Több helyettesítés használata, betűnként eltérő helyettesítés

- 1466 Alberti: Alberti titkosító korong / formula
  - Két korong: külső stabil (nyílt szöveg) és egy belső forgó (titkosított szöveg). A külső korongon számok is vannak, ezek kódtárban lévő szavakat jelölhetnek
  - **Titkosító ABC váltás tetszőleges helyen!**

  - Titkosítás 1. módszer:
    - Az helyettesítő ABC-t nagy betűk jelölik a titkosított szövegben.

  - Titkosítás 2. módszer:
    - A helyettesítő ABC váltása akkor következik be, amikor számot dekódolunk. Az első betű jelöli az helyettesítő ABC-t.

Többábécés titkosítás (folyt.)

- Johannes Trithemius (német)
  - *1499: Steganographia*
    - *Könyv a szteganográfiáról*
  - 1518: Polygraphia
    - Az első nyomtatott könyv a titkosításról
  - Tabula recta
    - A betűk kódolása a táblázat alapján

Kulcs

Titkosítandó betű

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

Tabula recta példa

- Kulcs: F
- Nyílt: G

- Titkos: L

Többábécés titkosítás (folyt.)

- 1553 Giovan Battista Bellaso (olasz)
  - “Vigenère cipher” De ezt nem ő találta fel!
  - A „tabula recta” alkalmazása úgy, hogy a helyettesítő ABC külön kulccsal van jelölve. Több variációt is publikált. Neki is volt „autokey” titkosítója, ahol a nyílt szöveg kezdőbetűi voltak a helyettesítő ABC kijelölői.

    - Nyílt: `ATTACKATDAWN`
    - Kulcs: `LEMONLEMONLE`
    - Titkos: `LXFOPVEFRNHR`

- 1586 Blaise de Vigenère (francia)
  - „Autokey” titkosító
    - Egy rövid kulcsszó után a nyílt szöveget használja a titkosító kulcsnak

    - Nyílt: `ATTACKATDAWN...`
    - Kulcs: `QUEENLYATTACKATDAWN...`
    - Titkos: `QNXEPVYTWTWP...`

Kevert titkosító ábécék (*Mixed cipher alphabets*)

- A titkosításhoz tetszőleges konverziót használhatok, de:
  - Egyértelmű legyen, azaz egy sorban és egy oszlopban csak egyszer forduljon elő ugyanaz a betű
    - Minden betűnek szerepelnie kell
- Hasonló, ha a oszlopokat és sorokat permutálom és Vigenere marad
- Célszerű egy adott eljárással képezni az egész titkosító táblázatot, és nem elküldeni azt
  - Kisebb méret, könnyebb kezelni

Kevert titkosító ábécék (folyt.)

- A kulcsszó meghatározza a kódolási táblázat ABC-jét.
  - Jelszóból képezhető, a jelszó adja meg a táblázat első betűit ismétlés nélkül. A táblázat többi része az alap ABC ismétlés nélkül
    - Pl.: CRYPTOGRAPHIC
CRYPTOGAHIBDEFJKLMNQSUVWXZ
  - Lehet a kulcsszón kívül az ABC képzés is kulcsos
    - Mátrixok, számmal kulcsolt mátrix, különböző kiolvasási útvonalak mátrixokban
    - Kulcs alapján minden valahányadik karakter kiolvasása

Kevert titkosító ábécé példák

Keyword— ARTILLERY

Keyword mixed sequence in matrix:

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

A jelszó adja meg az első sort, ez után a többi sort a jelszóban nem létező betűk adják. Kiolvasás oszlopok szerint.

Resulting sequence:

ABKURCMVTDNWIFOXLGPZEHQYJS

Keyword– CALIFORNIA

Hasonlóan az előbbihez, de a kiolvasásnál az oszlopok meg vannak keverve. Ez egy második kulcs.

2	1	5	4	3	7	8	6
C	A	L	I	F	O	R	N
B	D	E	G	H	J	K	M
P	Q	S	T	U	V	W	X
Y	Z						

Resulting sequence:

ADQZCBPYFHUIGTLESNMXOJVRKW

Keyword— TEXAS

In by rows:

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

Out spirally:

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

Kiolvasás spirálban

ZRMHBTEXASGLQYWVUNICDFKPOJ

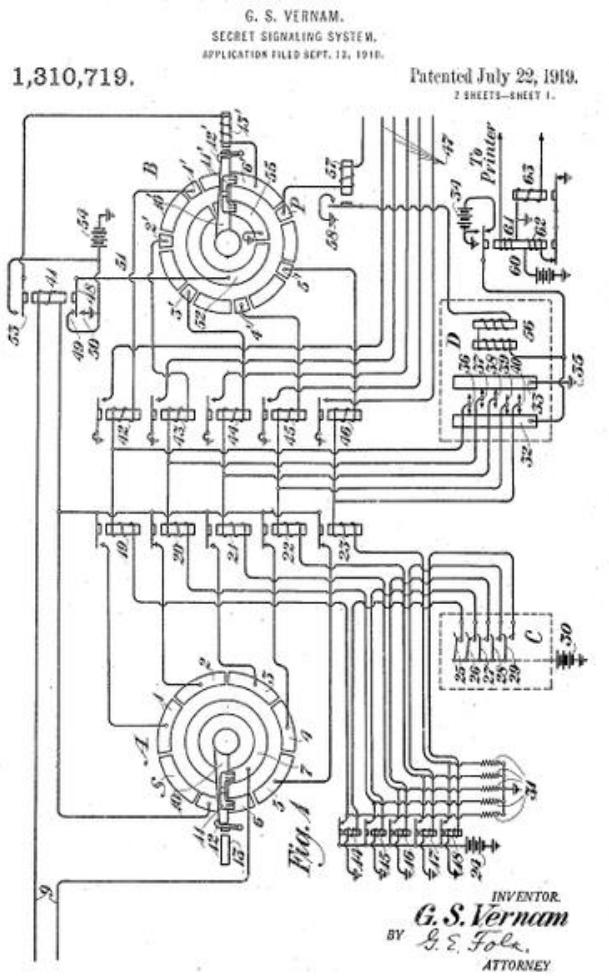
Többábécés titkosítás feltörése

- A korlátozott számú titkosító ABC miatt sérülékeny
  - Tabula recta esetén, ahány betűs ABC, annyi titkosító
  - Gyakoriság vizsgálat nem működik, mert nem tudom melyik betű melyik ABC-vel van.
    - Ugyanazon kulcs (ABC) alapján kódolt betűknél működik
    - Először a kulcs hosszát kell megtalálni (ahol ez jellemző), aztán a kulcs betűit
    - Babbage's (angol) módszer (1854)
    - Kasiski (porosz) módszer (1863)
      - Bigram vizsgálat

Kulcshossz meghatározása

A kriptográfia története
I. világháború

- One time pad (OTP)
  - 1917 Gilbert Stanford Vernam (AT&T) találta fel
    - Távíróhoz (TTY) találta ki. Egy papírszalagos kulcs és a nyílt/titkos üzenet
    - Az algoritmus relékkel megvalósítva (a mai XOR)
    - Nyílt: A = "++−−−“
    - Kulcs: B = "+−−++“
    - Titkos: G = "−+−++”
  - 1920 Joseph Oswald Mauborgne (amerikai)
    - A kulcs véletlen kell, hogy legyen
  - A kulcs tárolására jegyzetlapokat használtak (pad)

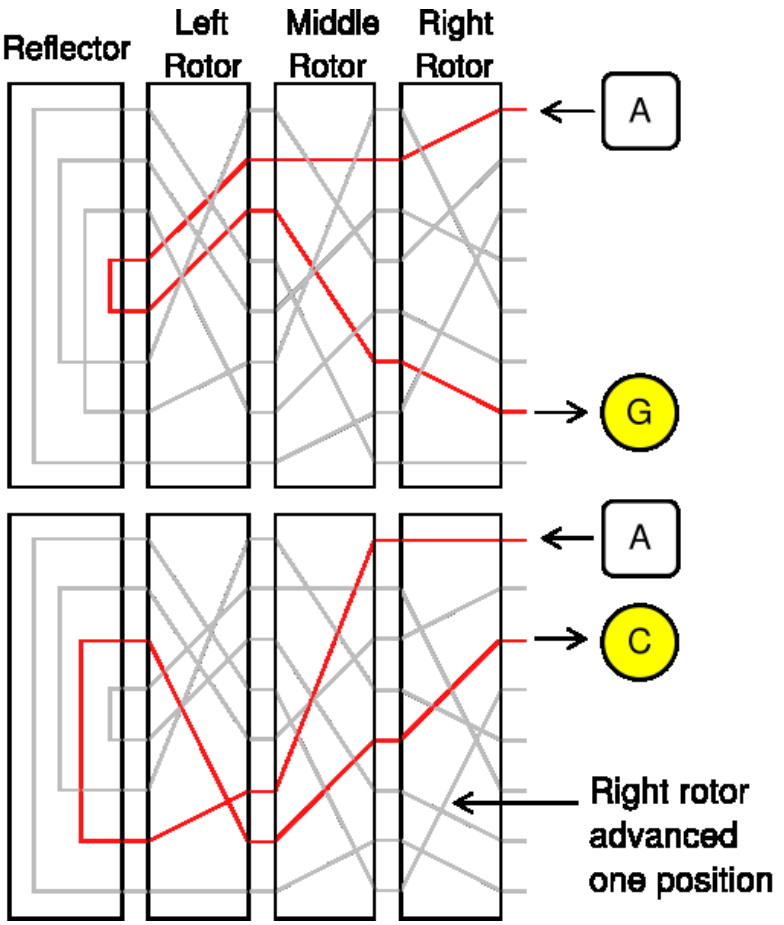


A kriptográfia története
II. világháború

- Mechanikus és elektromechanikus titkosító gépek
  - Németek: Enigma (1920) - rotor machine
  - Japán: Purple – stepping switch
  - Angol: TypeX – rotor machine
  - USA: SIGABA – rotor machine

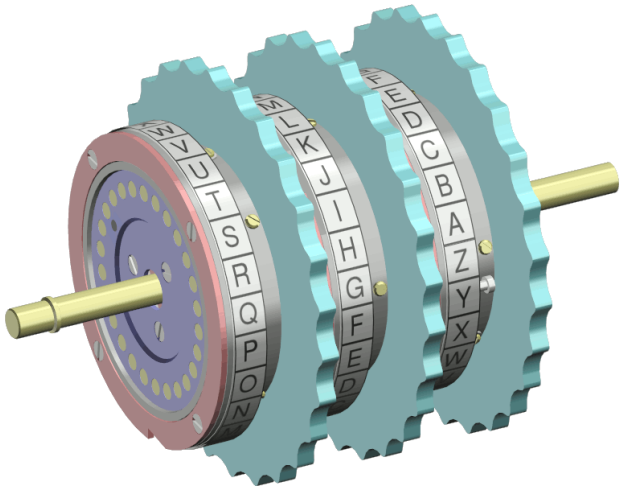
Rotor

- Komplex többábécés helyettesítés
  - A rotorok segítségével csinálják a helyettesítést
  - Több rotor
    - 3 rotor, 26 betű
    - 26^3 -> 17576 különböző összekötési variáció
  - Minden leütés után automatikus rotor léptetés (pozíciótól függően több is)



ENIGMA

- Rotor alapú titkosító gép
  - Tárcsák ABC gyűrűvel
  - 3-4 tárcsa hely, de több tárcsából választva
- Kapcsolótábla átkötések
  - Tetszőleges betűk kicserélhetőek. Tárcsás titkosítás előtti és utáni csere.
  - 1939-től 10 csere (max 13)



- Kulcs:
  - Tárcsák kiválasztása (~2^7), ABC gyűrű pozíciója (~2^9), tárcsa kezdő pozíciója (~2^{14}), kapcsoló tábla átkötés (~2^{47}) -> **2^{77} kulcs**

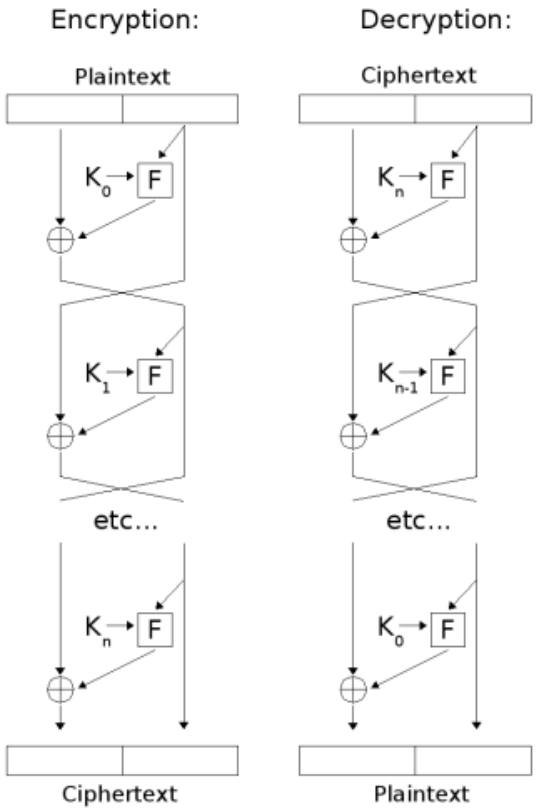
- Sok hibás döntés és elhagyott megerősítés miatt feltörhető volt.

A kriptográfia története
Modern kriptográfia

- Claude Shannon: Communication Theory of Secrecy Systems (1949)
    - A kriptográfia és kriptoanalízis elméleti alapjai
  - Nincs többé ábécé, csak bitek és bájtok
- 1975: DES – Data Encryption Standard: blokk titkosító
  - Horst Feistel
- 1976: Diffie-Hellman key exchange: kulcscsere
  - Bailey Whitfield Diffie és Martin Edward Hellman
- 1977: RSA: aszimmetrikus blokk titkosító
  - Ron Rivest, Adi Shamir és Leonard Max Adleman
  - 1973 Clifford Cocks (UK) lényegében ugyanezt feltalálta
- 1987: RC4: folyamtitkosító
  - Ron Rivest
- 1991: DSA – Digital Signature Algorithm: elektronikus aláírás
  - David W. Kravitz
- 1998: AES – Advanced Encryption Standard: blokk titkosító
  - Joan Daemen and Vincent Rijmen

1975/77: Data Encryption Standard

- DES születése
  - Horst Feistel (IBM)
  - 1970: NIST pályázat szabványos titkosítóra
  - 1977 január: nyertes DES: módosított Feistel cipher
  - 64 bites blokk titkosító, 56 (64) bites kulcs (8 paritás bit)
  - 16 kör (stages), 16 db 48 bites alkulcs
  - S-box és P-box: helyettesítés és permutáció
- Biztonság
  - Feltörés nyers erő módszer alapján
    - 1997 DES Challenge: 96 days
    - 1998 DES Challenge II-1: 41 days
    - 1998 DES Challenge II-2: 56 hours ($250.000 cost)
    - 1999 DES Challenge III: 22 hours 15 minutes
- 3DES
  - Megerősített biztonság, 112 bites kulcs, 3x lassabb működés (még ma is megtalálható)



Feistel Cipher

1976: Diffie-Hellman kulcscsere

- Aszimmetrikus tulajdonságokra épülve
  - Diffie-Hellman (-Merkle)
  - Eljárás
    - **p** prím és **g** generátor, $2 \leq g \leq p-2$
      - (1) A → B : $g^x \bmod p$
      - (2) A ← B : $g^y \bmod p$
      - x és y véletlen, $1 \leq x, y \leq p-2$
      - Közös kulcs: $K = (g^x)^y \bmod p = (g^y)^x \bmod p$
    - Csak a lehallgatás ellen véd!
    - Nincs közbeékelődéses támadás ellen védelem

Nyilvános kulcsú titkosítás

- Kulcspár használata:
  - $C=E_K(P)$, $P=D_{K^*}(C)$ vagy $C=E_{K^*}(P)$, $P=D_K(C)$
- A publikus kulcs mindenki számára ismert
- A privát kulcsot csak a felhasználó ismerheti

- Aszimmetrikus titkosítás

1977: RSA

- Ron **R**ivest, Adi **S**hamir, Len **A**dleman (MIT)
- A legelterjedtebb aszimmetrikus titkosítás

- Titkosítás (digitális aláírásra is használható)
  - Publikus kulcs: e, privát kulcs: d, modulus: n
    - $c = m^e \bmod n$
    - $m = c^d \bmod n$

n két hatalmas prím szorzata, nem tudjuk kiszámolni a két prímet
$d \cdot e \equiv 1 \pmod{\varphi(n)}$

Aszimmetrikus titkosítás

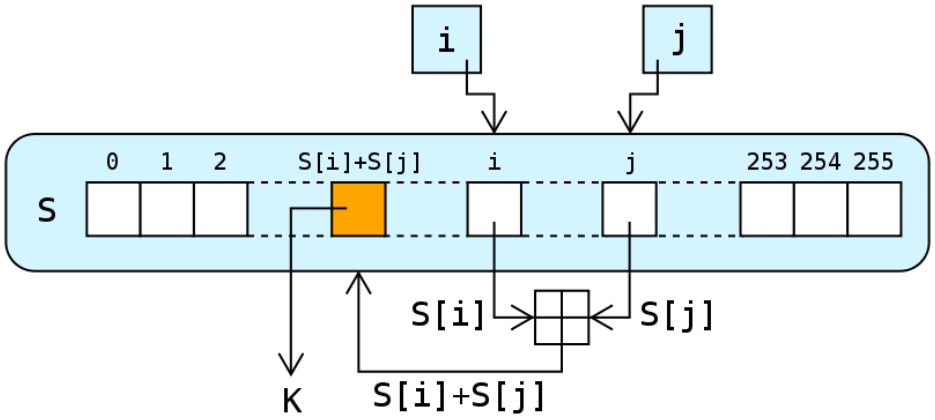
- Az RSA nagyon lassú
  - Csak a szimmetrikus kulcsot titkosítjuk vele! (128-256 bit)

- Léteznek gyorsabb megoldások, jelenleg ez irányba haladunk
  - El Gamal titkosító
  - Elliptikus görbe alapú kriptográfia

NIST javaslata az egyes kriptorendszerek kulcshosszának összehasonlítására:			
ECC modulus	AES	RSA modulus	RSA:ECC
112	56	512	5:1
161	80	1024	6:1
256	128	3072	12:1
384	192	7680	20:1
512	256	15630	30:1

1987: RC4 titkosítás

- RC4 – Ron's Code 4
  - Folyamtitkosító



- Inicializálás

```
for i = 0 to 255:
   S_i = i;
   j = 0;
   for i = 0 to 255:
      j = (j + S_i + K_(i mod l)) mod 256
      swap S_i, S_j
```

- Kulcsfolyam generálás

```
i = (i + 1) mod 256
j = (j + S_i) mod 256
swap S_i, S_j
Out = S[(S_i + S_j) mod 256]
```

C = P XOR K

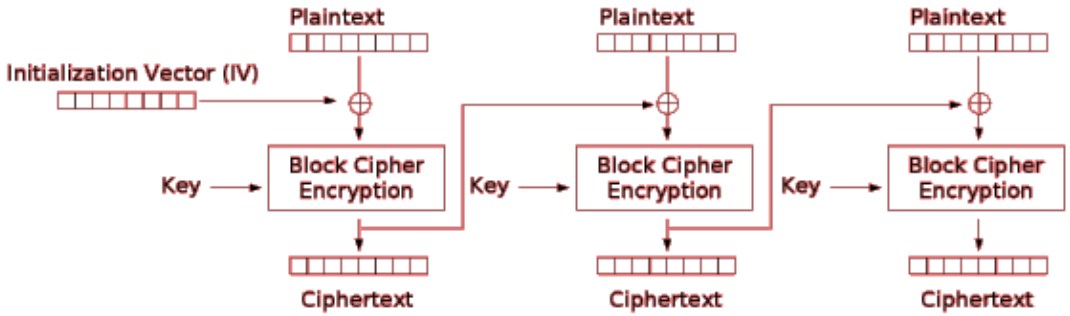
P = C XOR K

1998: AES – Advanced Encryption Standard

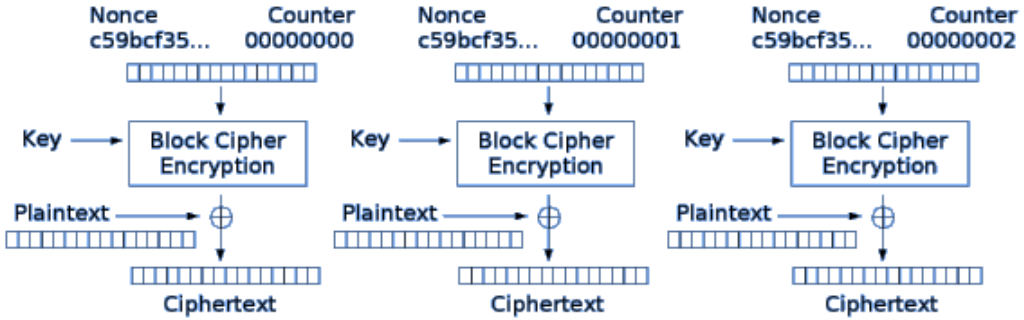
- Joan Daemen és Vincent Rijmen: Belga tudósok
- Substitution-permutation network
- 4x4 bájtos tömbökön dolgozik
  - AddRoundKey, SubBytes, ShiftRows, MixColumns
  - Az egyes lépések leírhatóak táblázatokkal is
  - 128 bites kulcs: 10 kör, 196 bites kulcs: 12 kör, 256 bites kulcs: 14 kör

CBC és CTR(ICM)

- Cipher Block Chaining / Counter Mode



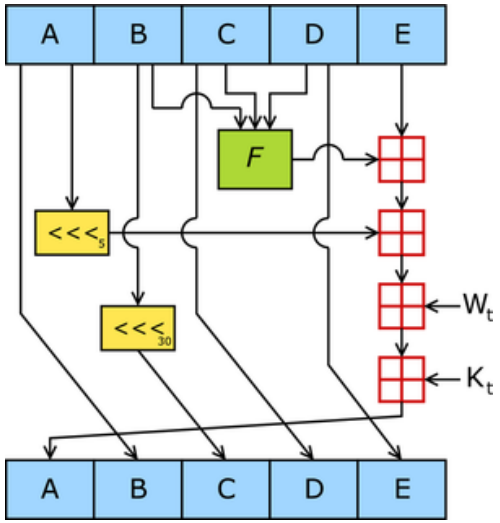
Cipher Block Chaining (CBC) mode encryption



Counter (CTR) mode encryption

SHA algoritmusok

- Secure Hash Algorithm
- 1993: SHA (SHA-0)
  - Hiba: collision in 2^{39} steps (2005)
- 1995: Secure Hash Algorithm – SHA-1
  - MD4 alapok
  - NIST javaslat
  - 160 bit hash kimenet (512 bit belső blokk)
  - Hiba: collision in 2^{69} steps (2005), 2^{61} steps (2012)
- 2001: SHA-2: SHA-224, 256, SHA-384, SHA-512
  - Ugyanaz a Merkle-Damgarg motor, mint az SHA-1
  - Biztonságosnak tartják ma is
- 2012(2014): SHA-3: Keccak
  - Fontos volt, hogy alapvetően más legyen



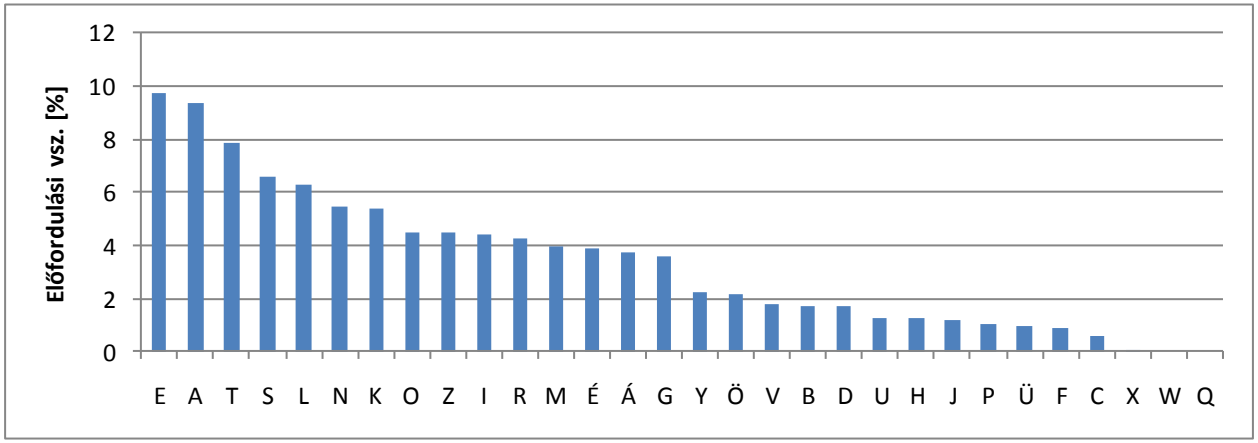
Kriptoanalízis

- A titkosítás megfejtése

- Helyettesítő titkosítás
  - Egyábécés (monoalfabetikus)
  - Többábécés (polialfabetkius)

Egyábécés titkosítás megfejtése

- A természetes nyelvekben jellemző az egyes betűk előfordulási valószínűsége
  - A titkos szövegben betűgyakoriság elemzéssel megállapítható a leggyakoribb betűk helyettesítője
  - A gyakori betűk megfejtése után a többi betű már adódik



Egyábécés titkosítás megfejtése (folyt.)

- A megfejtéshez gyakran rendelkezésre áll betűcsoportok valószínűsége is, amely szintén jellemző a nyelvre.
  - 1 betűs szavak, 2 betűs szavak
  - 2 vagy 3 betű egymás mellett

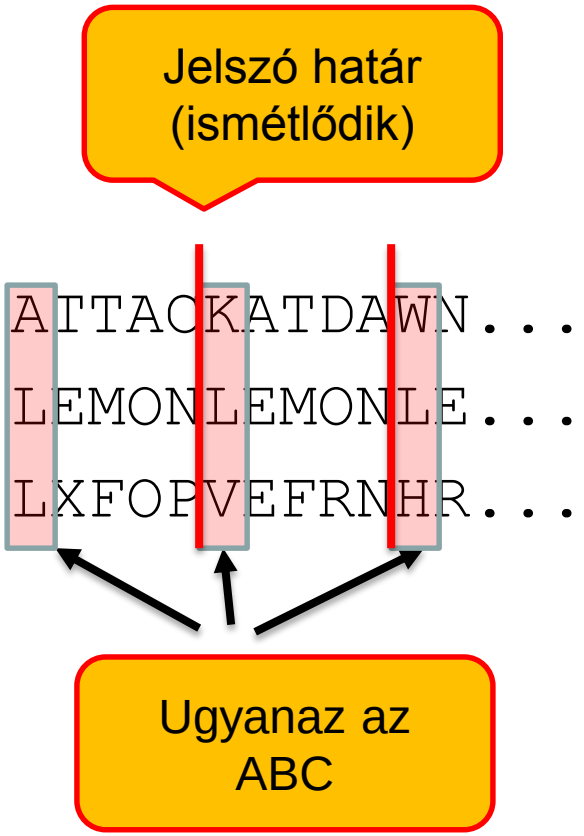
Többábécés titkosítás megfejtése

- Ha visszavezethető több egyábécés titkosításra, akkor már törhető

- Titkosításnál jelszó alapján ABC változtatás
  - Jelszó hosszának megfejtése
    - Egybeesések vizsgálata
    - Kasiski vizsgálat
  - Gyakoriságvizsgálat a jelszó hosszának megfelelően, külön csoportokban

Többábécés titkosítás megfejtése (folyt.)

- Nyílt:
- Kulcs:
- Titkos:



Titkosítás példa

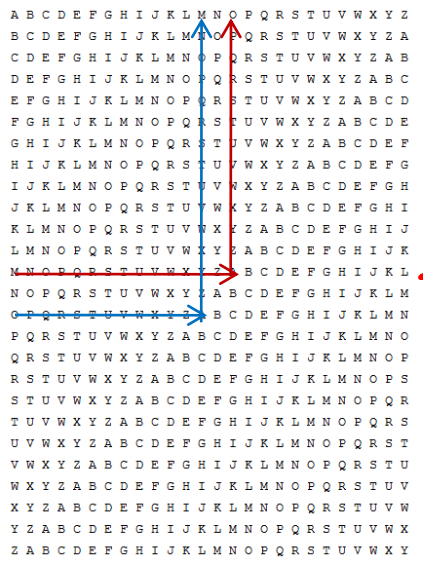
- Titkosított szöveg

VKMHG QFVMO IJOII OHNSN IZXSS CSZEA WWEXU
LIOZB AGEKQ UHRDH IKHWE OBNSQ RVIES LISYK
BIOVF IEWEO BQXIE UUIXK EKTUH NSZIB SWJIZ
BSKFK YWSXS EIDSQ INTBD RKOZD QELUM AAAEV
MIDMD GKJXR UKTUH TSBGI EQRVF XBAYG UBTCS
XTBDR SLYKW AFHMM TYCKU JHBWV TUHRQ XYHWM
IJBXS LSXUB BAYDI OFLPO XBULU OZAHE JOBDT
ATOUT GLPKO FHNSO KBHMW XKTWX SX

(forrás: www.murky.org)

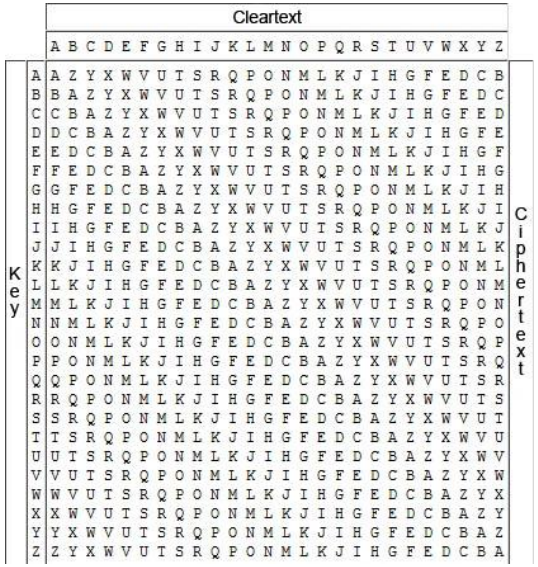
Titkosítás példa (folyt.)

- A kódoláshoz Beaufort titkosító (Sir Francis Beaufort)
  - Hasonló a Vigenere titkosítóhoz
    - (1. verzió) Más táblát használunk
    - (2. verzió) Máshogy használjuk a Vigenere táblát
  - A titkosító művelet azonos a titkosítás feloldásával



A kulcsnál felfelé fordul az irány

Ekvivalens tabula recta



Jelszó hosszának megfejtése

- Egybeesések vizsgálata (method of coincidences)
  - Ha eltoljuk a titkosított szöveget és megszámoljuk a karakter egyezéseket az eredetivel, akkor néhány karakter egyezni fog. A gyakoribb karakterek esetén az egyezés is gyakoribb, ha pont a jelszó hosszával vagy annak többszörösével történik az eltolás.

```
Eredeti:    VKMHGQFVMOIJOIIOHNSNIZXSSCSZEA...
Shift 1:    KMHGQFVMOIJOIIOHNSNIZXSSCSZEAW...   8
Shift 2:    MHGQFVMOIJOIIOHNSNIZXSSCSZEAWW...   12
Shift 3:    HGQFVMOIJOIIOHNSNIZXSSCSZEAWWE...   11
Shift 4:    GQFVMOIJOIIOHNSNIZXSSCSZEAWWEX...   13
Shift 5:    QFVMOIJOIIOHNSNIZXSSCSZEAWWEXU...   9
Shift 6:    FVMOIJOIIOHNSNIZXSSCSZEAWWEXUL...   25
Shift 7:    VMOIJOIIOHNSNIZXSSCSZEAWWEXULI...   11
```

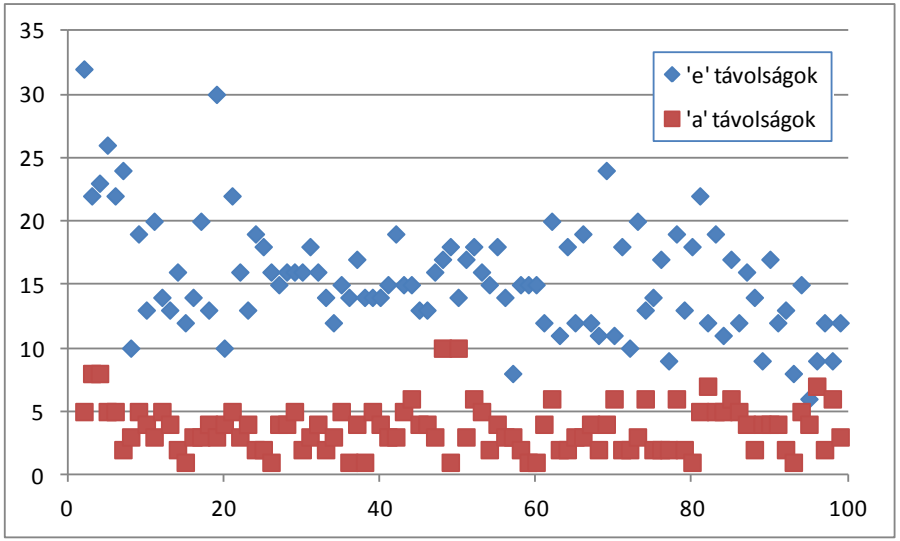
Egybeesések vizsgálata (folyt.)

- Magyarázat:
  - Az azonos távolságban lévő gyakori betűk száma jelentős
  - Ha a betűket kódoljuk, akkor a jelszó hossza szerinti távolságokban egyezést mutatnak
  - A véletlen egyezések száma kevesebb, mint az azonos betűk miatti egyezés

```
Nyílt:   MINEKNEVEZZELEK
Kulcs:   123123123123123
Titkos:  ASDWLDWXSPOSRWA
```

Petőfi: Minek nevezzelek

X: távolság
Y: gyakoriság

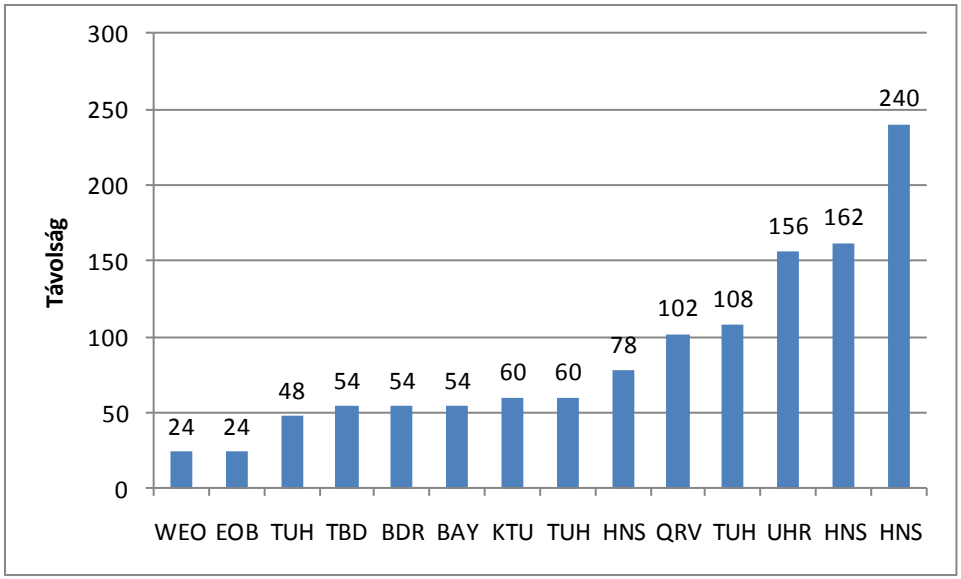


Jelszó hosszának megfejtése (folyt)

- Kasiski vizsgálat
  - Betűcsoportok előfordulását vizsgáljuk. A gyakran előforduló betűcsoportok (pl.: titkosított *the*) távolsága a jelszó hosszának többszöröse. Az esetleges véletlen egybeesés miatti tévedéseket figyelmen kívül kell hagyni.

Jelszó hosszának megfejtése (folyt.)

VKMHG QFVMO IJOII O**HNS**N
IZXSS CSZEA WWEXU LIOZB
AGEKQ UHRDH IKHWE OBNSQ
RVIES LISYK BIOVF IEWEO
BQXIE UUIXK EKTU**H** **NS**ZIB
SWJIZ BSKFK YWSXS EIDSQ
INTBD RKOZD QELUM AAAEV
MIDMD GKJXR UKTUH TSBGI
EQRVF XBAYG UBTCS XTBDR
SLYKW AFHMM TYCKU JHBWV
TUHRQ XYHWM IJBXS LSXUB
BAYDI OFLPO XBULU OZAHE
JOBDT ATOUT GLPKO F**HNS**O
KBHMW XKTWX SX



Legnagyobb közös osztó: 6

Jelszófüggő gyakoriságvizsgálat

- Egyábécés kódolások a jelszónak megfelelően

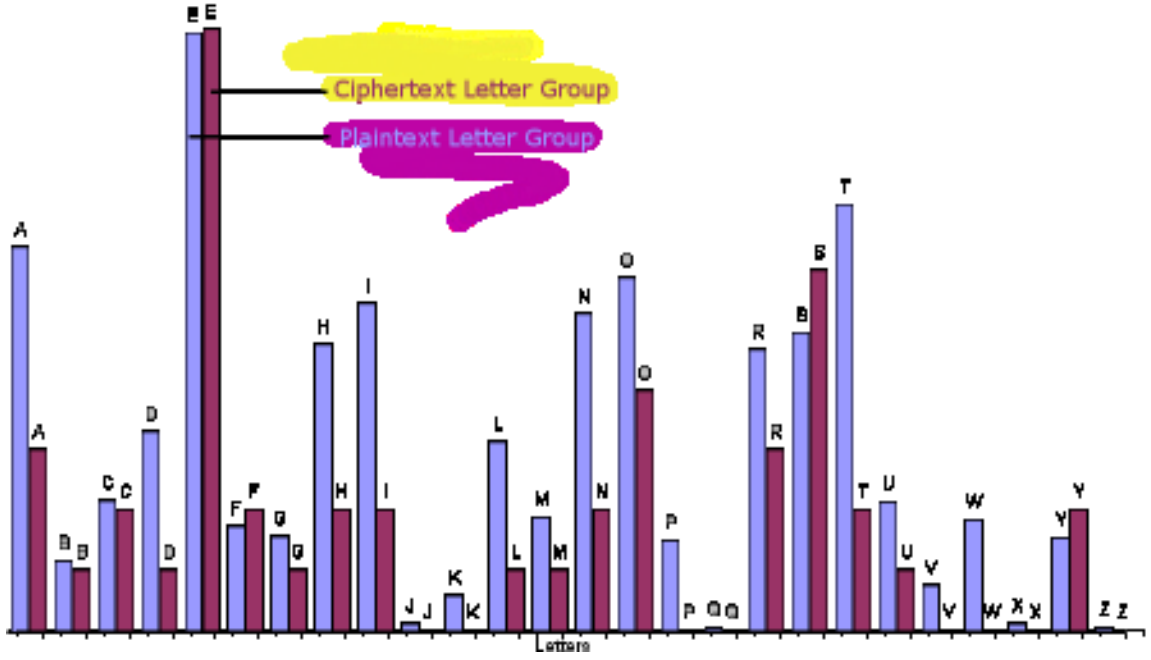
Annyi egyábécés csoport, ahány betű a kulcsban. Minden *x*. betű az (*x mod hossz)*. csoportba kerül, mert ezeket ugyanazzal a kulccsal titkosították!

```
0: VFOSSWIEDERIOEEESJFSIKLEDUSRYSSFCWQISYPUJTPSWS
1: KVINCWOKHOVSVOUKZIKENOUVGKBVGXLHKVXJXDOOOOKOXX
2: MMIISEZQIBIYFBUTIZYITZMMKTGFUTYMUTYBUIXZBUOKK
3: HOOZZXBUKNEKIQIUBBWDBDAIJUIXBBKMJUHXBOBADTFBT
4: GIHXEUAHHSSBEXXHSSSSDQADXHEBTDWTHHWSBFUHTGHHW
5: QJNSALGRWQLIWIKNWKXQREAMRTQACRAYBRMLALLEALNMX
```

Jelszófüggő gyakoriságvizsgálat (folyt.)

- Példa: az első karakter vizsgálata
  - Vizsgáljuk az egyes karakterek gyakoriságát

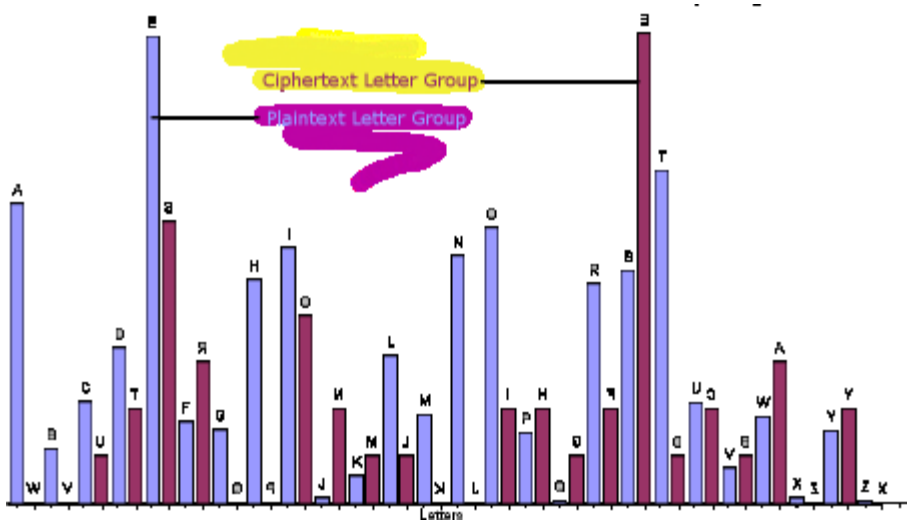
Hihetnénk, hogy nem Beaufort (mintha Vigenere lenne). Mivel viszont az, ezért ez így biztosan nem jó, nem csak a leggyakoribbakat kell vizsgálni!



Jelszófüggő gyakoriságvizsgálat (folyt.)

- Az összes lehetséges eloszlást (A helyettesítő ábécék szerint) megvizsgáljuk és keressük a legkisebb eltérést
  - Pl.: négyzetes különbség

Jelszó: **W**OMBLE



Megfejtés

```
BEAUF ORTAN DVIGE NEREB ECOME MUCHE ASIER
TOANA LYSEW HENTH EREIS ALOTO FTEXT TOWOR
KWITH THISA LLOWS USTOU SETHE REPEA TINGN
ATURE OFTHE KEYTO OBTAI NMANY VALUA BLEST
ATIST ICSON CETHE LENGT HOFTH EKEYI SASCE
RTAIN EDORP ERHAP SGUES SEDAT THENG ROUPS
OFLET TERSA KEYLE NGTHA PARTC ANBEA NALYS
EDASI FTHEY WEREA CAESA RCIPH ER
```

- "Beaufort and Vigenere become much easier to analyse when there is a lot of text to work with. This allows us to use the repeating nature of the key to obtain many valuable statistics. Once the length of the key is ascertained or perhaps guessed at, then groups of letters a key length apart can be analysed as if they were a Caesar cipher"

Az önkulcsoló (autokey) titkosító feltörése

- A nyílt szöveg megjelenik a kulcsban

- Példa Vigenere autokey titkosítót használva

```
Nyílt üzenet:   MEETATTHEFOUNTAIN
Kulcs:          KILTMEETATTHEFOUN
Titkos üzenet:  WMPMMXXAEYHBRYOCA
```

Az önkulcsoló (autokey) titkosító feltörése (folyt.)

- Gyakori szavak keresése (Pl.: THE)
  - titkosított: WMP MMX XAE YHB RYO CA
  - Kulcs próba: THE THE THE THE THE ..
  - nyílt: DFL TFT **ETA FAX** YRK ..

  - titkosított: W MPM MXX AEY HBR YOC A
  - Kulcs próba: . THE THE THE THE THE .
  - nyílt: . TII TQT HXU **OUN** FHY .

  - titkosított: WM PMM XXA EYH BRY OCA
  - Kulcs próba: .. THE THE THE THE THE
  - nyílt: .. WFI EQW LRD IKU VVW

Feltesszük, hogy a „the” szó valahol szerepelni fog a szövegben. Nem tudjuk hol. Ezért mindenhol próbálkozuk.

- A nyílt szöveg darabkák előfordulási valószínűség szerint rendezése
  - (valószínű) FAX OUN ETA … … FTF DFL EQW (valószínűtlen)

Az önkulcsoló (autokey) titkosító feltörése (folyt.)

- A jelszó hosszának kitalálása (remélhetőleg nem túl hosszú)
  - Hossz 3: Látszik, hogy nem jó.
  - Hossz: 4:

```
titkos:     WMPMMXXAEYHBRYOCA
kulcs:      ......ETA.THE.OUN
nyílt:      ......THE.OUN.AIN
```

  - Hossz: 5:

```
titkos:     WMPMMXXAEYHBRYOCA
kulcs:      .....EQW..THE..OU
nyílt:      .....THE..OUN..OG
```

  - Hossz: 6:

```
titkos:     WMPMMXXAEYHBRYOCA
kulcs:      ....TQT...THE...O
nyílt:      ....THE...OUN...M
```

Itt megint olyan darabok vannak, amik valószínűleg jók

A kulcs miatt itt ez a nyílt szöveg

A nyílt szöveg használata miatt itt ez a kulcs

Az önkulcsoló (autokey) titkosító feltörése (folyt.)

- Lehetséges kulcs/nyílt szöveg keresése

```
titkos :    WMPMMXXAEYHBRYOCA
kulcs:      ..LTM.ETA.THE.OUN
nyílt:      ..ETA.THE.OUN.AIN
```

- A nyílt szöveg megfejtése
  - Mivel a nyílt szöveg megjelenik a kulcsban, ezért rögtön visszajelzést is kapunk

```
nyílt: M.ETA.THE.OUN.AIN
nyílt: MEETATTHEFOUNTAIN
```

Az önkulcsoló titkosító feltörése II.

- Gyakoriság vizsgálat használata
  - Önkulcsoló titkosító esetén is lehet használni a visszafejtett nyílt szövegen keresztül

- Példa:

```
VFPJUDEEVUHCUWRNGSZNKARFFNVXILDPFNVXI?ANLBDHYUBYV
GYAIXDSMXKFBPITVXDUYNWWTTPIZVUITXOYBXQENNTXMJQKHM
FBTJZBHBFLHZYKOLFOJFQISQQJHNPCYKDKYAWQYFIIHMDSFFE
RJGSDFJQZJWTWNFG?FNSSDYQRUXKSFVKVSUZCRFZIKFUEKVIE
ZFFLPIZYHTSBTRYJELFSDUNQMYVHW?VXKCRFCAQZHCPENQSGP
EXZUFXQLYVZUAEIVGLYNEIIFKXQJZWLPLVYWBTNURIALZAGVK
NTDMTQHEKYCOZYTEFGNZUYTXOSQLAATPIIAVALTZXROPKZSNX
QJWJWWJJRGEFGAOIRXLLGDLBBFDRP
```

(forrás: Vorlath blog)

- Itt már nem a megszokott titkosító táblát használjuk!

Az önkulcsoló titkosító feltörése II. (folyt.)

Példa:
Jelszó: KRYPTOS

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

Az önkulcsoló titkosító feltörése II. (folyt.)

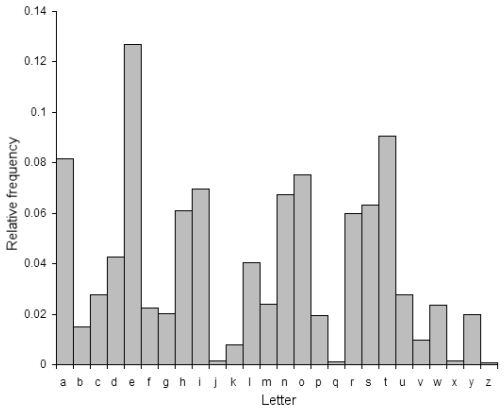
- A megfejtéshez tudnunk kell
  - A rejtéshez használt ABC táblát
  - A kulcsszó hosszát
    - A korábban ismertetett módszerek itt nem használhatóak, ugyanis a kulcsban nincs ismétlődés!
- Találgatás módszere

Az önkulcsoló titkosító feltörése II. (folyt.)

- Ismert ABC és kulcshossz (találgatással)
  - A kulcs minden egyes betűjére külön próbálkozunk. Csoportokat képzünk a kulcs hosszának megfelelően.
    - *n* hosszú kulcs esetén: 1., n+1., 2n+1., … betűk
  - A csoportok a kulcsot + a potenciális nyílt szöveget tartalmazzák, az összes (26: angol ABC) esetre. Minden egyes kulcsszó betűre külön csoport
  - A csoport következő betűje a nyílt szöveg megfelelő betűje és a csoportban előtte lévő betűvel, mint kulccsal van kikódolva

Az önkulcsoló titkosító feltörése II. (folyt.)

- A kialakuló csoportokban, amelyek már a nyílt szöveg részeit tartalmazzák, az előforduló betűk gyakoriságát vizsgáljuk. Mennyire jellemző a nyílt ABC-re?
  - A gyakoriság vizsgálatnál a betűket egy értékkel jelöljük, azok nyílt szövegben lévő súlyuk szerint
    - Pl.: angolban:
      ABCDEFGHIJKLMNOPQRSTUVWXYZ
      84779657812768628896553 60
  - A legtöbb pontot elért a legvalószínűbb megoldás



Az önkulcsoló titkosító feltörése II. (folyt.)

- A példában a kulcsszó hossza 8
- A példa alapján az első betűcsoport
  - 1., 9., 17., 25., … betűk visszafejtve
    - 1. betű:
      - titkos: V, kulcs: A -> nyílt: I
    - 9. betű:
      - titkos: V, kulcs: I -> nyílt: A
    - …

Az önkulcsoló titkosító feltörése II. (folyt.)

- Az összes betűre megnézve

```
1 AIASSSYEGENOHTTGANNNWIOUTEHHONSAGYGTIXVSVESNTCTZ 350
2 BTLITIUANLFNERERNLXGASURHWOECLWSEERYNPENENEUYOO  348
3 SWLBHBSREDOWRADUUODLBTLIEHKEAYATXIESUOSONDITFNX  330
4 CAYLALETTXRAENUUNCOEOHDERENXTWSMTGEETIERTEGEODX  353
5 ISIETEDHITMSDSNNKAEYUEIDEROAIWHEHHSVENCTYGHSUSY  350
6 STNHPTTSCHAGAMDDNTSKTYTOSEWCOTISITFESTOHSRTFRWI  356
7 SOVOOHHMFETANIETOILNTSSUOXSTNHSSRDINSFNSEEMOSEZ  354
8 ATIWSEEAIIITDTROWOAOHHBTMWTLOILATEFMIIDEVEIRESU  358
```

- Az első betűk kiadják a kulcsszót, a többi pedig a nyílt szöveg
  - (A kulcsszó mentén olvasva: It was totally…)

Statisztikai tesztek

- Statisztikai tesztek segíthetnek a kriptoanalízis során

- Egyezések vizsgálata (Index of coincidence)
  - Ha két véletlen angol (latin) betűt összehasonlítunk, akkor az egyezés 1/26 = 0.0385 valószínűségű
  - Ha angol szövegből, két véletlen pozíció alapján választott betűt hasonlítunk össze, akkor az egyezés valószínűsége 0.0667 (empirikusan)
    - **Nem egyezik a véletlen összehasonlítással!**
  - Különböző tesztekben (próbák) ezt ki tudjuk használni

Példa:
ALM**A**
123**4**

Index of coincidence

- William Friedman: *The Index of Coincidence and its Applications in Cryptography (1920)*

- φ_r: Egy *c* elemű ABC esetében az *N* hosszúságú véletlen szövegben ***1/c ·N(N-1)*** a betűegyezések várható értéke
- φ_p: Amennyiben nem véletlenről van szó, úgy ***IC/c ·N(N-1)***, ahol *IC* az adott nyelvre jellemző
- φ_o: A tényleges előfordulás adott szövegben: $\sum \mathbf{n_i(n_i-1)}$

English	1.73
French	2.02
German	2.05
Italian	1.94
Portuguese	1.94
Russia	1.76
Spanish	1.94

ABRAKADABRA
12345678901

A: 5, B: 2, R: 2, K:1, D:1
A: 1-4,1.6,1-8,1-11,4-1,4-6.4-8,4-11,6-1,6-4,6-8,6-11,8-1,8-4,8-6,8-11,11-1,11-4,11-6,11-8
B: …

Index of coincidence

- ΔIC: A megfigyelt és a véletlen aránya

  $\varphi_o/\varphi_r = \frac{1}{1/c}\sum_{i=1}^{c}\frac{n_i(n_i-1)}{N(N-1)}$

Csak gyakoriságot vizsgálunk, mindegy, hogy milyen betűről van szó. Lehet titkosított is!

- Példa:

```
QPWKA LVRXC QZIKG RBPFA EOMFL  JMSDZ VDHXC XJYEB IMTRQ WNMEA
IZRVK CVKVL XNEIC FZPZC ZZHKM  LVZVZ IZRRQ WDKEC HOSNY XXLSP
MYKVQ XJTDC IOMEE XDQVS RXLRL  KZHOV
```

- Egy ABC vagy több ABC:
  - Megvizsgáljuk, hogy minden x. betű esetén a kapott csoportok lehetnek-e egy angol szöveg kódolt elemei
    - Eredmény:
      1:1.12, 2:1.19, 3:1.05, 4:1.17,**5:1.82**, 6:0.99, 7:1.00, 8:1.05, 9:1.16, 10:2.07

ΔIC példa 2.

Letters:	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
f:	3	3	0	7	2	1	1	4	0	0	1	0	0	0	4	1	6	3	0	4	1	0	5	1	0	3
f-1:	2	2		6	1			3							3		5	2		3			4			2
f(f-1):	6	6		42	2			12							12		30	6		12			20			6

$$\phi o = \Sigma f(f-1)$$
$$= 6 + 6 + 42 + 2 + 12 + 12 + 30 + 6 + 12 + 20 + 6$$
$$= 154$$

$$\phi p = .0667\, N(N-1)$$
$$= .0667 \times 50 \times 49$$
$$= 163$$

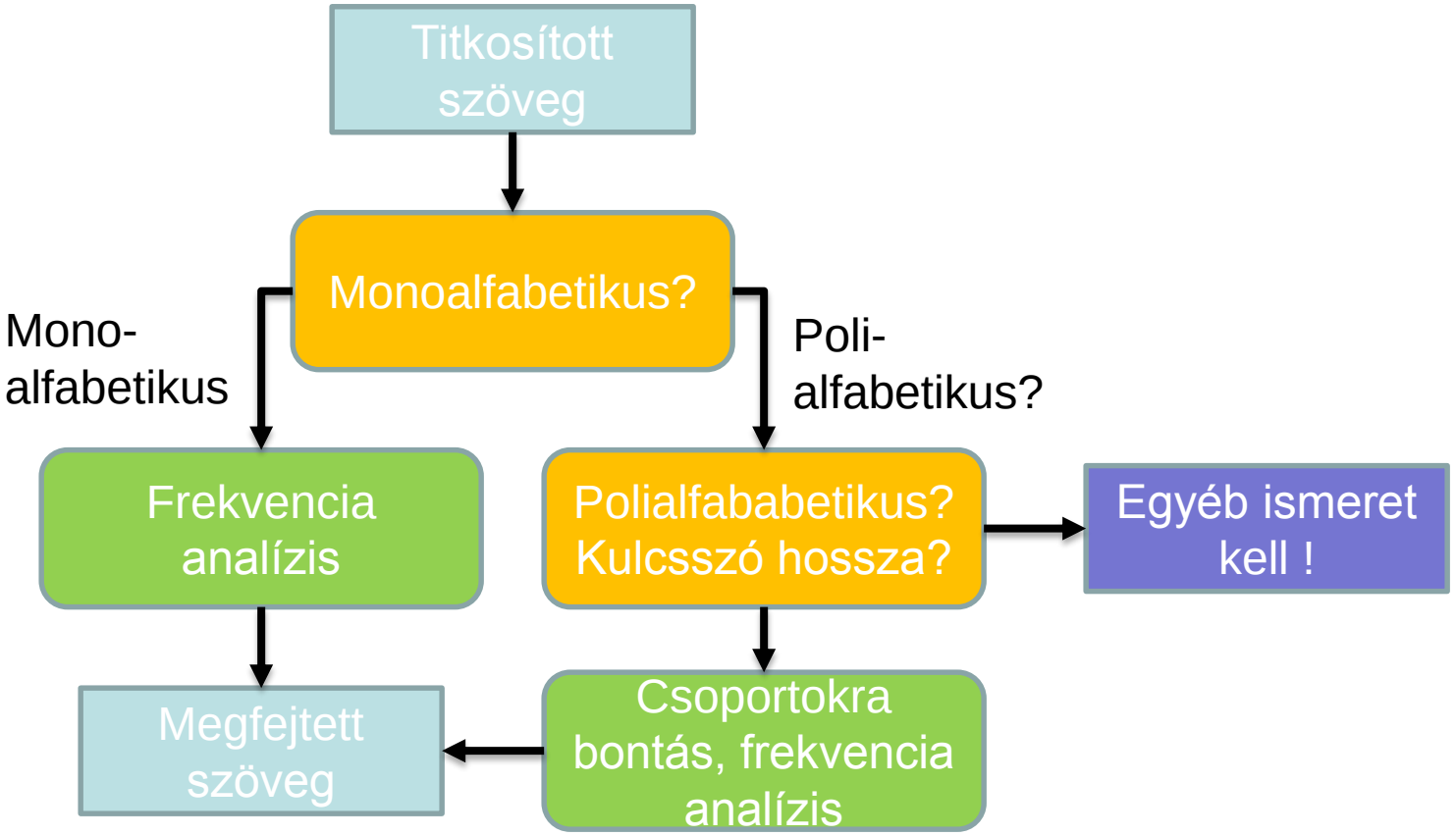
$$\phi r = .0385\, N(N-1)$$
$$= .0385 \times 50 \times 49$$
$$= 94$$

$$\Delta IC = \phi o / \phi r$$
$$= 154/94$$
$$= 1.64$$

Index of coincidence

- Felhasználható
  - Monoalfabetikus vagy polialfabetikus titkosítás
    - Betűhalmaz esetén is
  - Polialfabetikus esetén a kulcsszó hossza

Tikosítások vizsgálata



Irodalom

- US ARMY Cryptography manual
  - http://www.umich.edu/~umich/fm-34-40-2/