

Kriptográfia

Harmadik előadás Klasszikus titkosítások II

Dr. Németh L. Zoltán

SZTE, Számítástudomány Alapjai Tanszék

2008 ősz

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 ismétlődést
- 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 esetben 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,

$$0 \text{ XOR } 1 = 1 \text{ XOR } 0 = 1$$

$$0 \text{ XOR } 0 = 1 \text{ XOR } 1 = 0$$

A XOR művelet kedvező tulajdonságai

- XOR = „kizáró vagy” ($1 \text{ XOR } 1 = 0$ miatt)
 - Jeölni szokták még így: $\oplus$
 - Tulajdonságai:
 - $x \text{ XOR } y = y \text{ XOR } x$
 - $x \text{ XOR } (y \text{ XOR } z) = (x \text{ XOR } y) \text{ XOR } z$
 - $x \text{ XOR } x = 0$
 - $x \text{ XOR } 0 = x$
 - Ezért $(x \text{ XOR } y) \text{ XOR } y = x$, vagyis ha kétszer végezzük el a XOR-olást ugyanazzal az y -nal, visszacapjuk az eredeti x -et.
- A megfejtés és a titkosítás algoritmusai megegyeznek.

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 hozzáadáásos 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 hozzáadáásos módszernek
One-Time pad: OTP
- A OTP azért feltörhetetlen 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

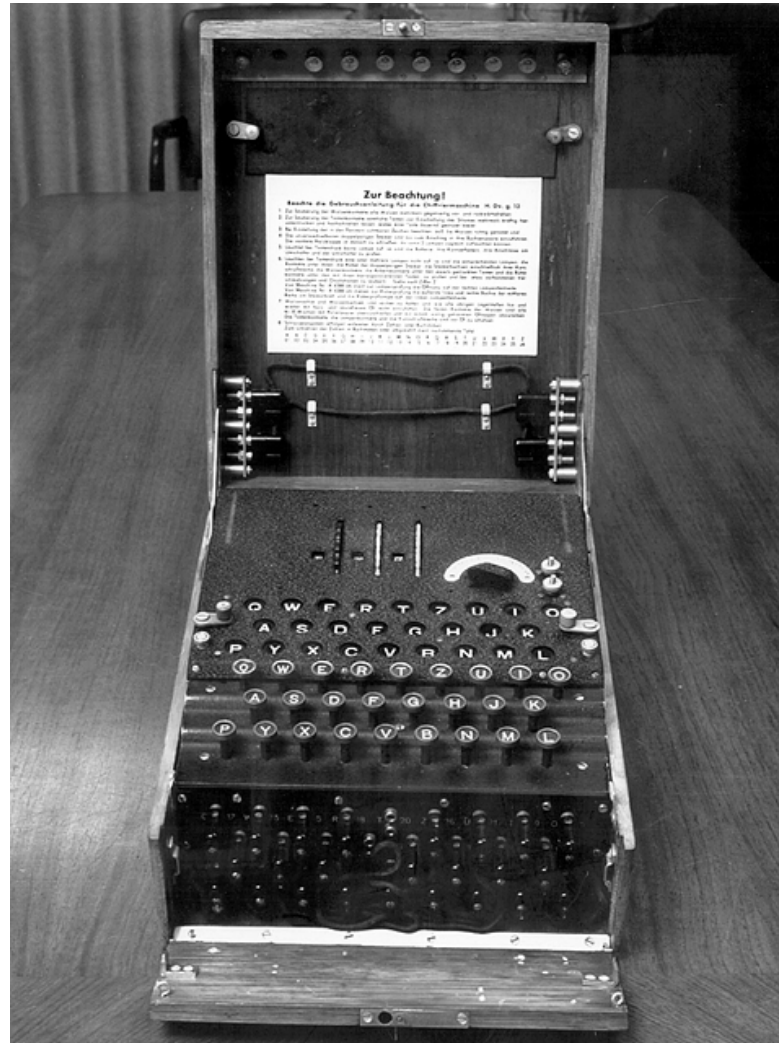
Alkalmazása

- Ezek a gyakorlati problémák alkalmazását erősen korlátozzák.
- Csak alacsony sáv szélesség 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](http://en.wikipedia.org/wiki/Numbers_station)

Rotoros gépek (Rotor Machines)

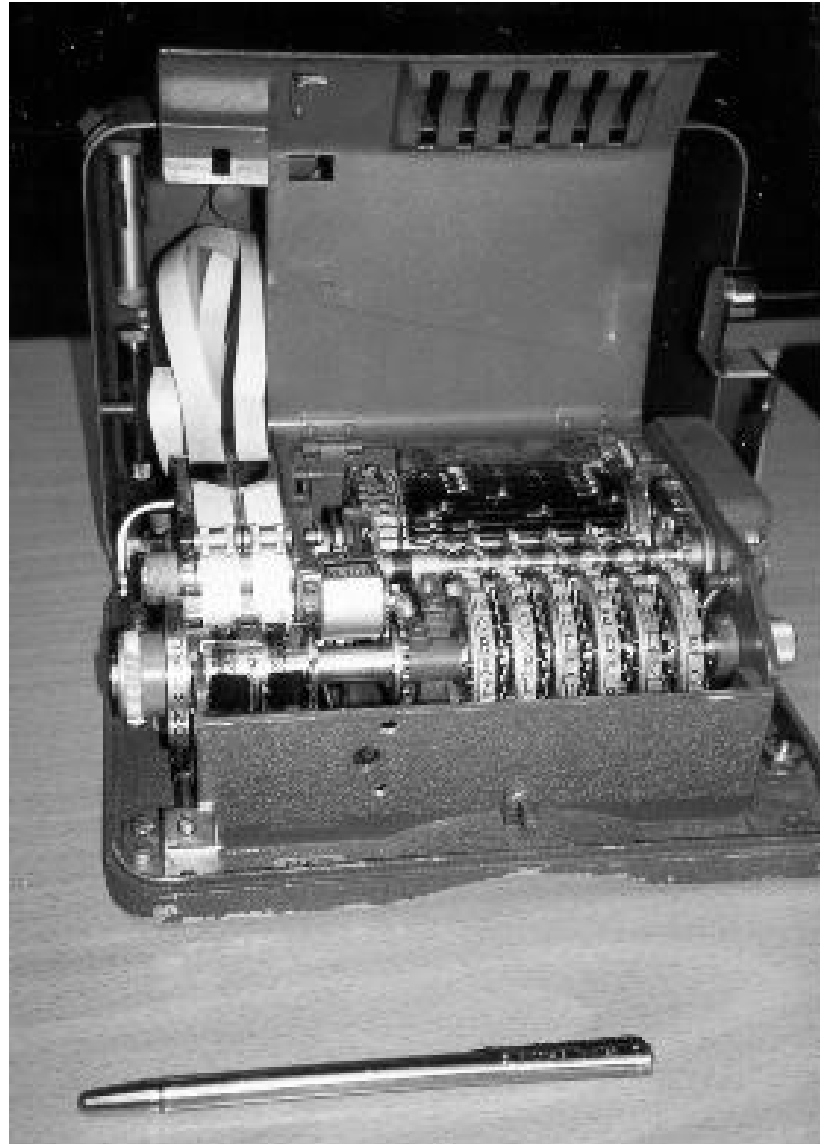
- a számítógépek és ezzel a modern titkosítók megjelenése előtt a rotoros gépek voltak a legelterjedtebb komplex titkosító eszközök
- Széles körben használták a II. világháboróban:
 - németek: Enigma, szövetségesek: Hagelin, japánok: Purple
- Igen bonyolult többábécés helyettesítések
- forgó korongok (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>

Közzölük 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 egységei (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:

MEMATRHTGPRYETEFETE0AAT

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**

Produkcións 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 generáció: kvantumelvű titkosítások, sikeres kísérletek 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)