Adatbiztonság, adatvédelem

Tantárgyi követelményrendszer, történeti áttekintés, bevezetés

Ki is vagyok én?

- Ruzsinszki Gábor – Mérnök – informatikus, tanár, író
  - Déri Miksa szakközépiskola
- E-mail:
  - ruzsinszkig@sziszszi.hu
  - webmaster442web@gmail.com
- Web: webmaster442.hu
- E-mail átfutási időm: 1-3 nap.
- Oktatott tárgyak: Adatbiztonság

Tantárgy információk

- 2 Kredit – 1 óra előadás 1 óra gyakorlat
- Elméleti tárgy inkább, ebből adódóan a gyakorlat is elmélet orientált.
- A gyakrolati órákon interaktív párbeszédet szeretnék megvalósítani feladat megoldással.
- Ehhez az kell, hogy ne legyenek hűek a nevükhöz, az-az ne csak hallgatók legyenek.

ZH, vizsga

- Aláírási követelmény: 3 pont megszerzése. A félév során 100 pont szerezhető
- Nem kötelező járni, de **erősen ajánlott**.
- 2 nagy ZH lesz gyakorlati időpontban – 40 pont / db
- Véletlenszerű időpontban kis ZH feladatok összesen 20 pontért

ZH, vizsga

- A két nagy ZH időpontja
  - Félév közepén
  - Félév végén
- A vizsga szóbeli lesz.
  - Tételsor legkésőbb a félév végig ki lesz adva
- Megajánlott jegy szerezhető 70 pont vagy több elérésével

Tantárgy információk

- Diák elérhetőek lesznek, tehát nem kell bajlódni a másolásukkal.
- Ez azonban **nem azt jelenti, hogy nem kell jegyzetelni** az előadás közben.
- Lusta vagyok diákat készíteni, sok minden szóban lesz elmondva*
- Előző féléves statisztika alapján a hallgatók 50%-a teljesítette a tárgyat úgy, hogy a hallgatók 50%-a nem jelent meg vizsgán

Miről szól ez a tárgy?

- Betekintés az Adatvédelem és adatbiztonság témakörökbe
- Csak alapozás, mivel igen nagy témakör
- A kurzus elvégzése != lever 9000 hacker minősítés
- A tananyag sikeres elsajátításához kellenek matematikai alapismeretek

Tervezett tematika

- Történeti áttekintés (Ma)
- Adatvédelmi megoldások általánosságban
- Titkosítás alapjai
- Hash algoritmusok működése
- Egykulcsos rendszerek: DES, AES és társaik
- Kétkulcsos rendszerek: RSA, PGP
- WLAN hálózatok biztonsága
- Beágyazott rendszerek biztonsága
- Szteganográfia
- Adatvédelmi törvény áttekintése

Az adatbiztonság és Adatvédelem rövid történeti áttekintése

A kezdetek…

- Tény: Mióta „civilizáltan” élünk, vannak háborúk.
- A vezetők által a katonáknak küldött üzenetek, adatok mindig is kiemelten fontosak voltak.
- Ezért az első adatvédelmi (titkosítási) módszereket a hadsereg fejlesztette/készítette.
- Ma is a legnagyobb fejlesztő a hadsereg.

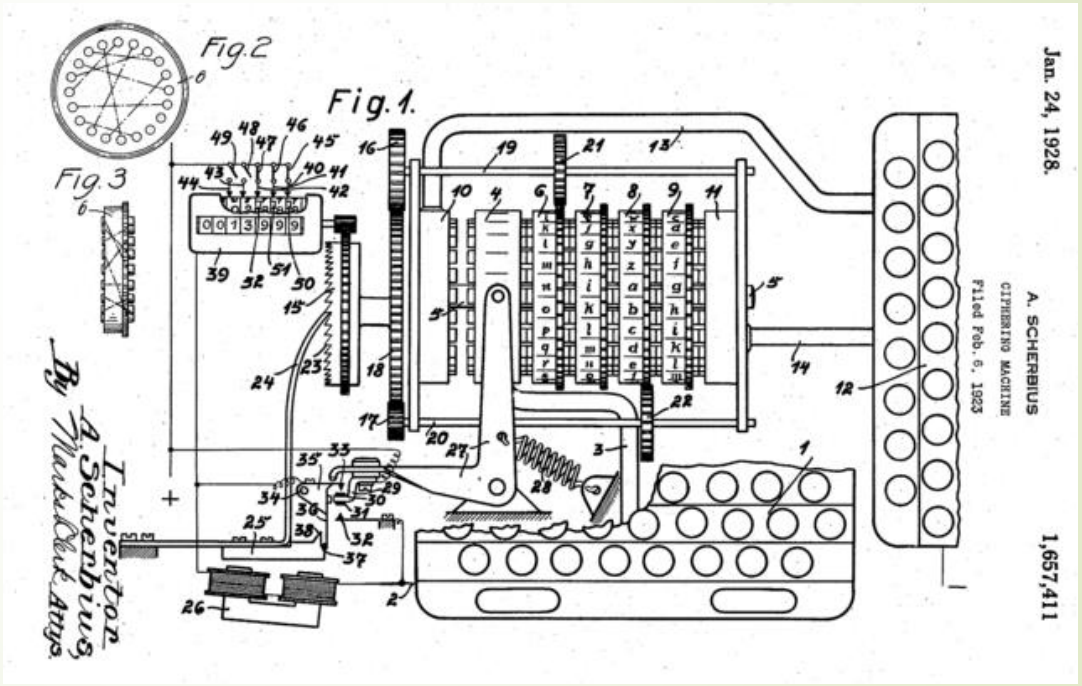
A XX. Század

- A II. világháború jelentős lökést adott a titkosítási módszereknek.
- Itt jelentek meg az első elektronikus titkosító berendezések.
- Így a visszafejtés miatt fejlődésnek indult a számítástechnika is.

A német csodagép, az Enigma

- Enigma: Görög eredetű szó, jelejtése: titkok, rejtvény.
- 1920-ban Arthur Scherbius találta fel.
- A németek által a második világháborúban használt titkosítási módszer.
- Papírra dolgozik, viszont gép nélkül nem fejthető vissza belátható időn belül.
- Elektromechanikus berendezés.

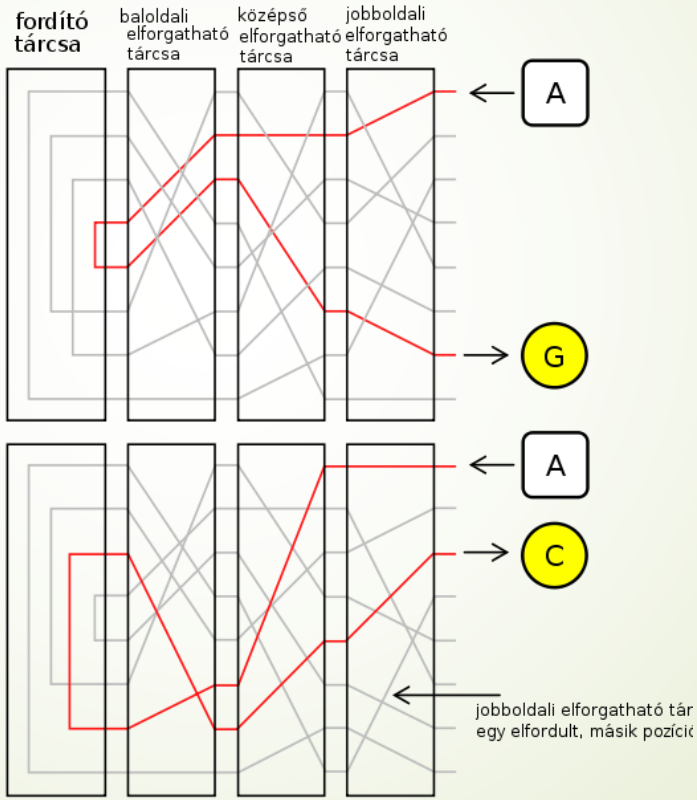
Az Enigma


Jan. 24, 1928.
A. SCHERBIUS
1,657,411
CIPHERING MACHINE
Filed Feb. 6, 1923
Fig. 1.
Fig. 2
Fig. 3
Inventor
A. Scherbius
By Munn & Co.
Attys.

Az enigma működése

- Titkosító kulcsos működésű.
- Tárcsák kódolják a betűket, minden egyes betű leütése átrendezi a tárcsák helyzetét a kulcs alapján.
- Egymás után titkosítva ugyanazt az üzenetet, nem kapunk azonos kódolt eredményt.
- Visszafelé is működik. Kódolt üzenetet újból titkosítva az eredeti üzenetet kapjuk meg.

A működése


fordító tárcsa
baloldali elforgatható tárcsa
középső elforgatható tárcsa
jobboldali elforgatható tárcsa
A
G
A
C
jobboldali elforgatható tár
egy elfordult, másik pozíci

Feltörése

- A háború tényleges kitörése előtt, 1932-ben már feltörték a kereskedelmi változatát. Ez még csak 3 tárcsát alkalmazott.
- A feltörés a lengyel Marian Rejewski nevéhez fűződik.
- Lengyelország megszállása előtt a francia és brit katonák kimentették az országból.

Feltörése

- A háború alatt alacsony prioritású üzenetek feltörésén dolgozott a hadseregnél.
- Feltörése a titkosítási algoritmus hibája miatt lehetséges (ezekről később lesz majd szó), pedig a kulcstere igen nagy.
- 3 tárcsa esetén lehetséges kulcsok száma: 3 498 626
- 10 tárcsa esetén (katonai változat): ~2,167 * 10^14

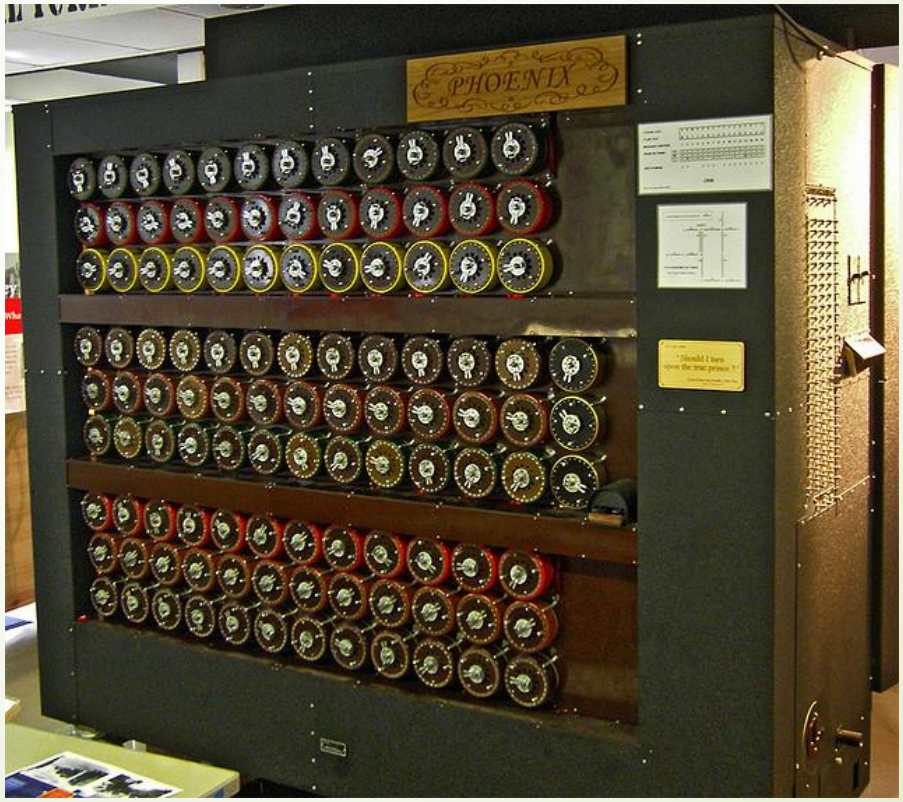
A feltörés gépesítése

- Rejewski eredményei alapján Alan Turing kifejlesztette a Turing Bombát.
- Ez egy elektromechanikus számítógép volt.
- Egy 10 tárcsával kódolt üzenetet nagyjából 6 óra alatt dekódolt egy gép.
- A gépek összekapcsolhatók voltak. Így 60 gép 6 perc alatt dekódolt egy üzenetet.
- A háború utolsó évében átlagosan 24 másodperc alatt dekódoltak egy üzenetet.

A feltörés gépiesítése

- A 24mp-es idő az üzenetekben Ismétlődő mintáknak köszönhetően volt lehetséges.
- A Turing bomba alapján alkotta meg Turing az általános Turing gép modellt.
- A modell 5 műveletet használ. Ha ezzel egy probléma megoldható, akkor annak a megoldására építhető gép.

A Turing Bomba



Ajánlott Film: Kódjátszma / The Immitation Game

A háború után

- Hadititok maradt, hogy sikerült feltörni a titkosítást (A háború ideje alatt is igen kevesen tudtak róla)
- Az első kereskedelmi Unix rendszerek még tartalmazták az Enigma titkosítást.
- Csak 1970-ben hozták nyilvánosságra, hogy a második világháború idején is meg tudták törni.

A titkosítás mai helyzete

- Nem csak katonai alkalmazás.
- Szinte mindennapos, bárki által elérhetőek különböző megoldások.
- Egyre kifinomultabb és jobb módszerek születnek meg.
- A félév folyamán lesz ezen megoldásokról szó részletesen és a történelmükről is.

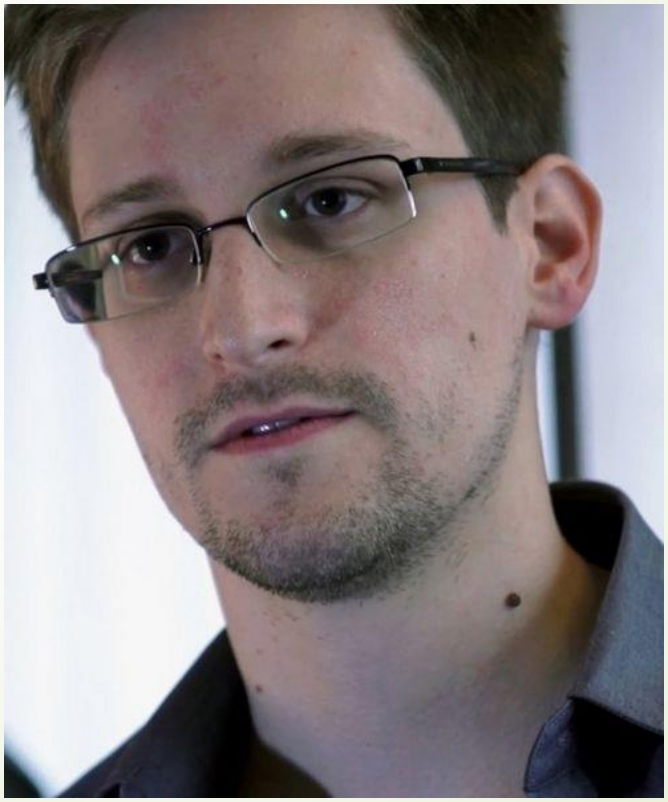
A titkosítás mai helyzete

- Amit titokban akarunk tartani, azt titkosítani kell.
- Köszönhetően a következőknek:
  - Snowden botrány
  - Magánélet / Privát szféra visszaszorulása az Internet és a közösségi oldalak előtörésével

Edward Snowden

- NSA alkalmazott volt.
- Információt szivárogtatott ki azzal kapcsolatban, hogy az NSA globálisan akit tud megfigyel és lehallgat különböző módszerekkel.
- Nagyon nagy botránynak kellett volna ebből lennie, de valahogy még sem lett az.

Edward Snowden



A Snowden ügy és amit tudni lehet róla

- Az NSA-nek nem kell végigjárnia a jogi utat adatkikérés esetén.
- Bejárásuk van minden Facebook, Gmail és Live fiókba.
- Az okostelefonok szoftvereit úgy módosították, hogy bárhol lehallgatható és bemérhető legyen a célszemély.

A Snowden ügy és amit tudni lehet róla

- A bemérés kikapcsolt telefon esetén is működik.
- Többek között ezért beépített az iPhone és sok egyéb telefon akkumulátora.
- Az NSA és CIA valamint az érintett cégek természetesen tagadnak mindent.

Az ügy hozadéka

- Még ha az állításainak nagy része csak rémhír, akkor is az ügy hozadéka mellett nem lehet elmenni szó nélkül.
- Ha a bizalom megrendült, akkor a bizalom meg van rendülve, amit nem lesz könnyű visszaállítani.
- Kényes adatokat többen fognak titkosítani, mint eddig
- Nagy technológiai cégek esetén nem kizárt a profit vesztés sem.

Az ügy hozadéka

- A hosszú távú következmények még nem láthatóak előre.
- Paranoiás, azonban helytálló gondolat: 2x gondoljuk meg, hogy mit teszünk közzé az interneten.

Köszönöm a figyelmet