Nyílt kulcsú rejtjelezés

Ötletek és alkalmazások

Miről lesz ma szó?

Mikor használunk titkosított üzeneteket?

Mit várunk egy titkosítási módszertől?

Korai és modern megoldások

Milyen matek teszi ezt lehetővé?

Hol találkoztok titkosítással?

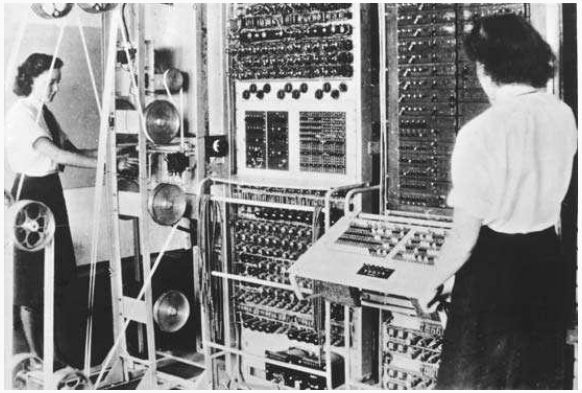
Privát üzenetek: Whatsapp, Gmail, Messenger

Banki tranzakciók: átutalások, Amazon, Paypal, Visa

Jelszavak kezelése: hogyan tárolja Facebook a jelszavamat?

Digitális aláírás: honnan tudjuk, hogy tényleg a feladótól jött az üzenet?

Online játékok: miért nem lehet csalni online pókerben sem?



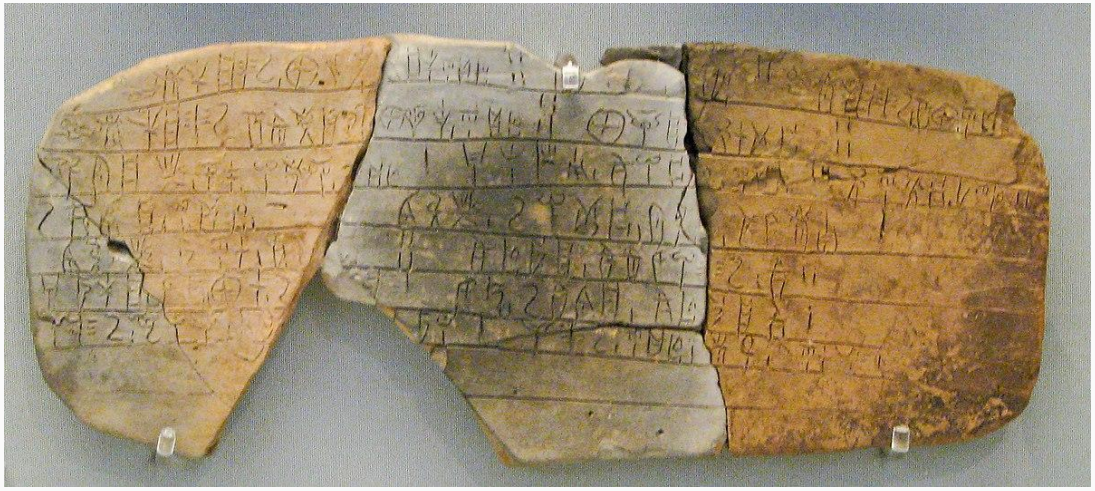
A Colossus Mark 2 számítógép és a kezelők (Women's Royal Naval Service), 1943

Mit várunk egy kripto rendszertől?

- privát kommunikáció két fél között
- a csatorna (internet) nem biztonságos
- a titkosítási módszer is publikus
- **a két fél nem ismeri egymást előzetesen?!**

1969-ben elkobzott kelet német R353 kém rádió szett és részben felhasznált OTP

Régészet és kódfejtés



Alice Kober és a Linear B táblák

A Cézár-kód

A B C D E F G H … L … X Y Z

X Y Z A B C D E … O … U V W

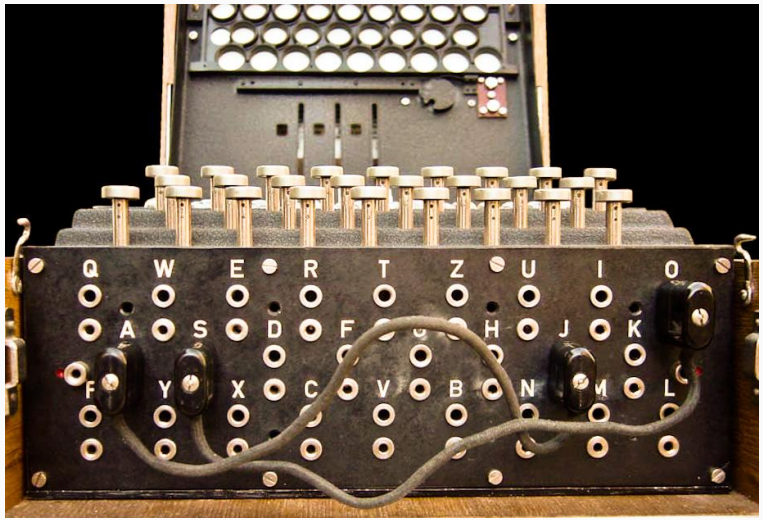
Pl: három betűvel eltolva az ABC

HELLO → EBOOR

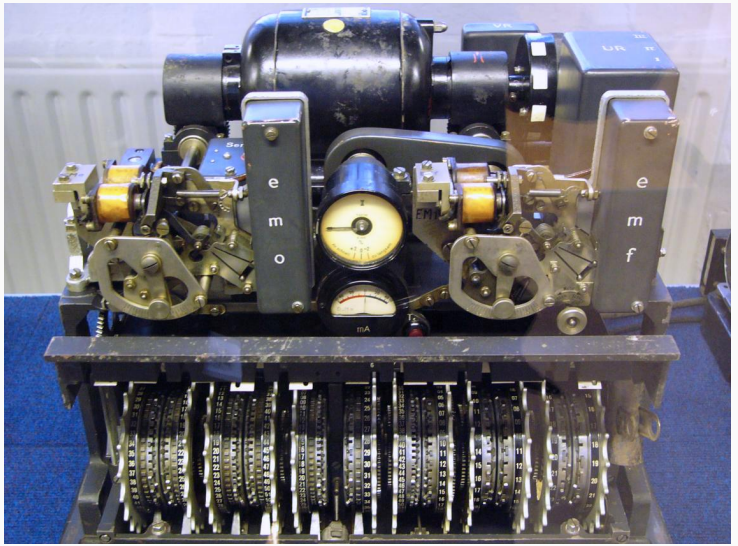
Mi a gyengéje ennek a módszernek?

Hogyan írhatunk le egy ilyen kódolást matematikailag?

Enigma és Lorenz kódolók az 1940-es évekből



By Bob Lord - German Enigma Machine, uploaded in english wikipedia on 16. Feb. 2005 by en:User:Matt Crypto, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=258976



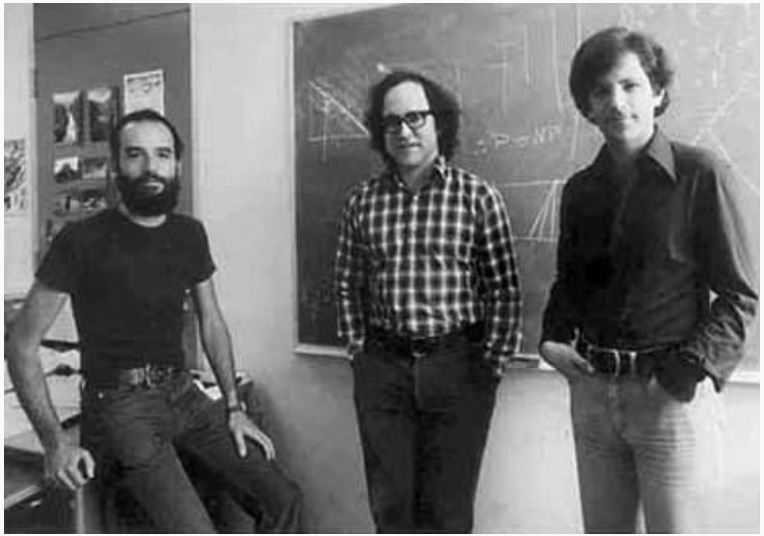
Mi a probléma az egykulcsos kódolással?

Egyirányú függvények

- Mi lehet egy **egyirányú függvény**?
- Példák esetleg?
- Ötletek alkalmazásra?

Merkle, Hellman és Diffie 1977-ben

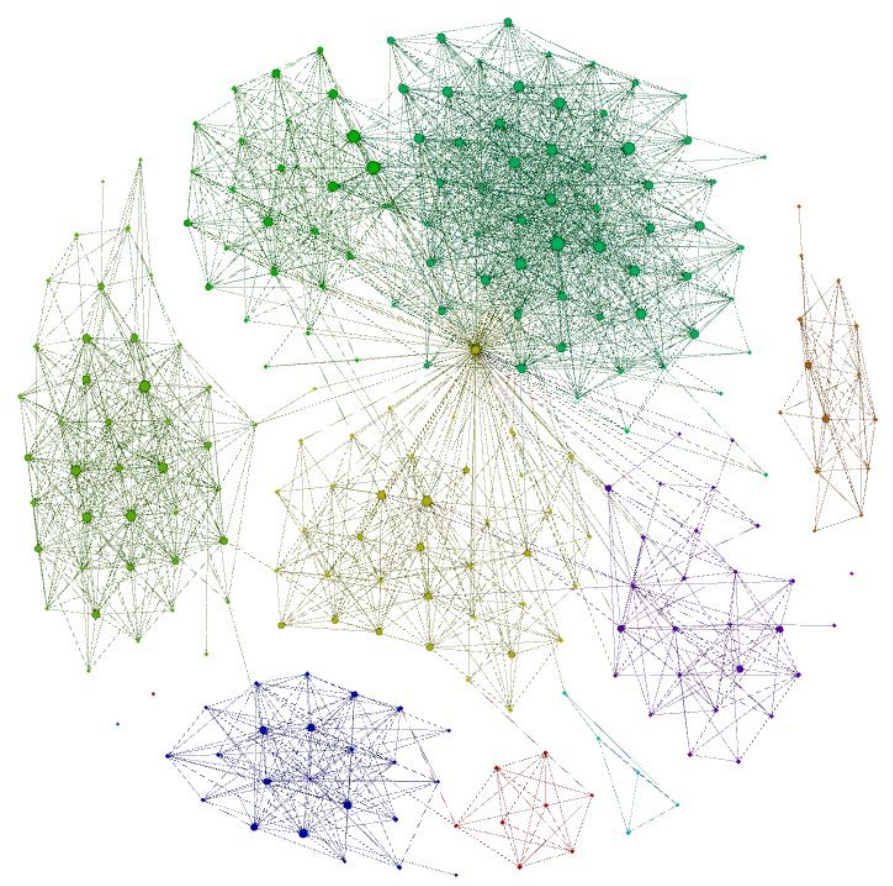
Alkalmazások



Shamir, Rivest és Adleman

- Jelszó menedzsment
- Elkötelezettségi sémák
- Digitális aláírás
- Nyílt kulcsos kódolás: RSA és változatai

Nyílt kulcsú kódolás gráfokkal



- Mik is a gráfok?
- Hogyan kódolhatunk egy számot?
- Hogyan dekódolhatjuk a számot?
- Komplexitás és sebesség

Egy Facebook baráti társaság gráfon
(http://allthingsgraphed.com)

Mire lennétek még kíváncsiak?

Köszi szépen!