Public-key cryptography

Ideas and applications

What are we talking about today?

When do we use secret messages?

What are we demand of a cryptographic system?

Early and modern solutions

What kind of math helps?

When do you encounter cryptography?

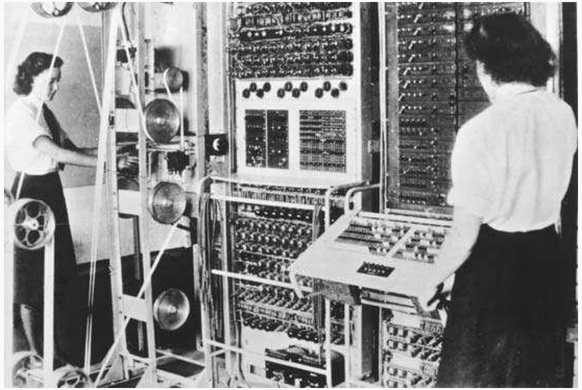
Private messages: Gmail, Whatsapp, Facebook

Bank transactions: Visa, Amazon, Paypal

Password management: how are passwords stored?

Digital signatures: how do we know that the message is coming from the real sender?

Online gaming: how is fair poker possible through the internet?



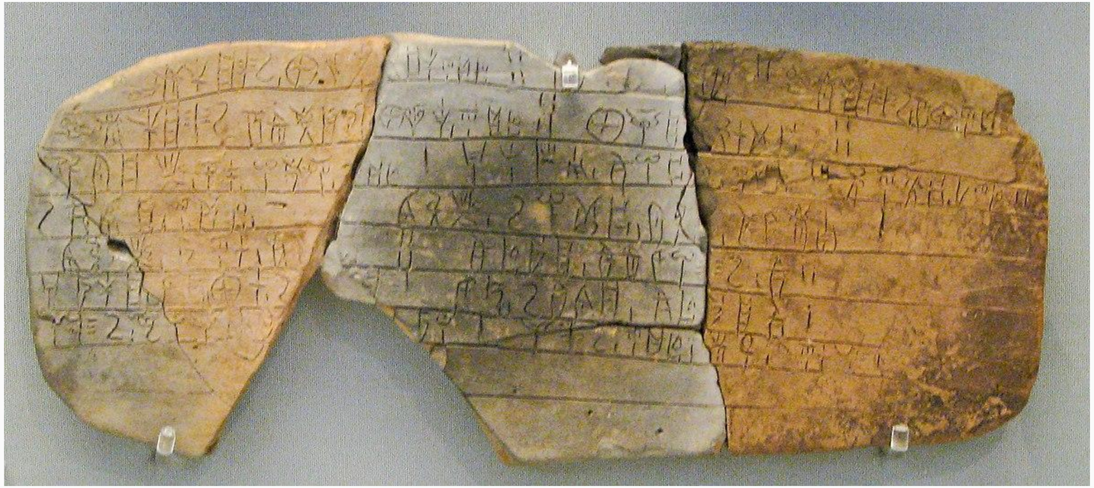
The Colossus Mark 2 computer and members of the Women's Royal Naval Service, 1943

What do we expect of a cryptosystem?

- Private communication between two parties
- The communication channel is unsecure
- The cryptographic technique is public
- **The parties have not met before?! No chance for an in-person key exchange...**

An East German R353 spy radio and one-time pad, confiscated in 1969 in the Netherlands

Deciphering ancient texts



Alice Kober and the Linear B tablets

The Caesar code

A B C D E F G H … L … X Y Z

X Y Z A B C D E … O … U V W

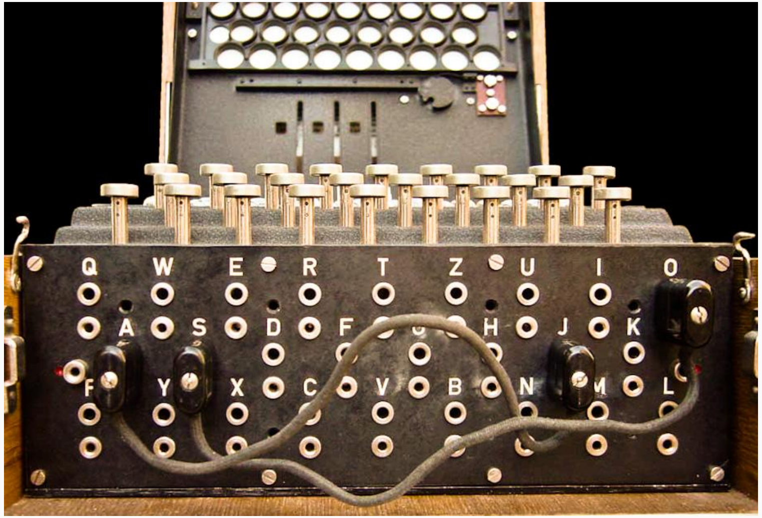
We translate the alphabet by 3 letters

HELLO → EBOOR

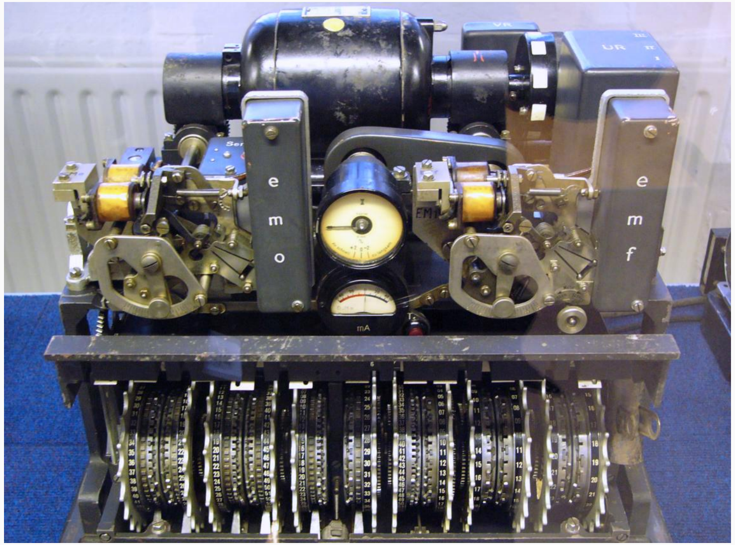
What are the weaknesses?

So what is a cryptosystem really?

The Enigma and Lorenz machines from the 1940s



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



What are the main problems with one-key cryptography?

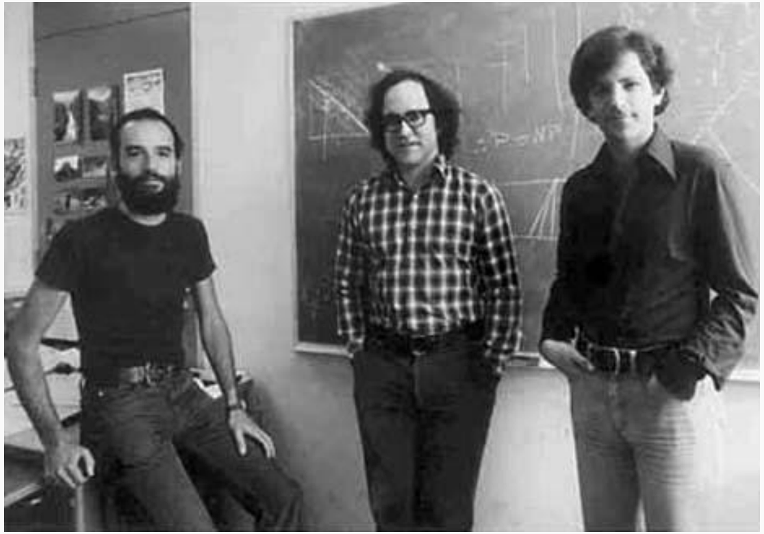
One-way functions

- What is a **one-way function**?
  - Going x to y=f(x): easy and fast,
  - Given y, finding x such that y=f(x): hard and slow

- Some examples: a dictionary, a phonebook, **the discrete log**, multiplication vs factorization.

Merkle, Hellman and Diffie in 1977

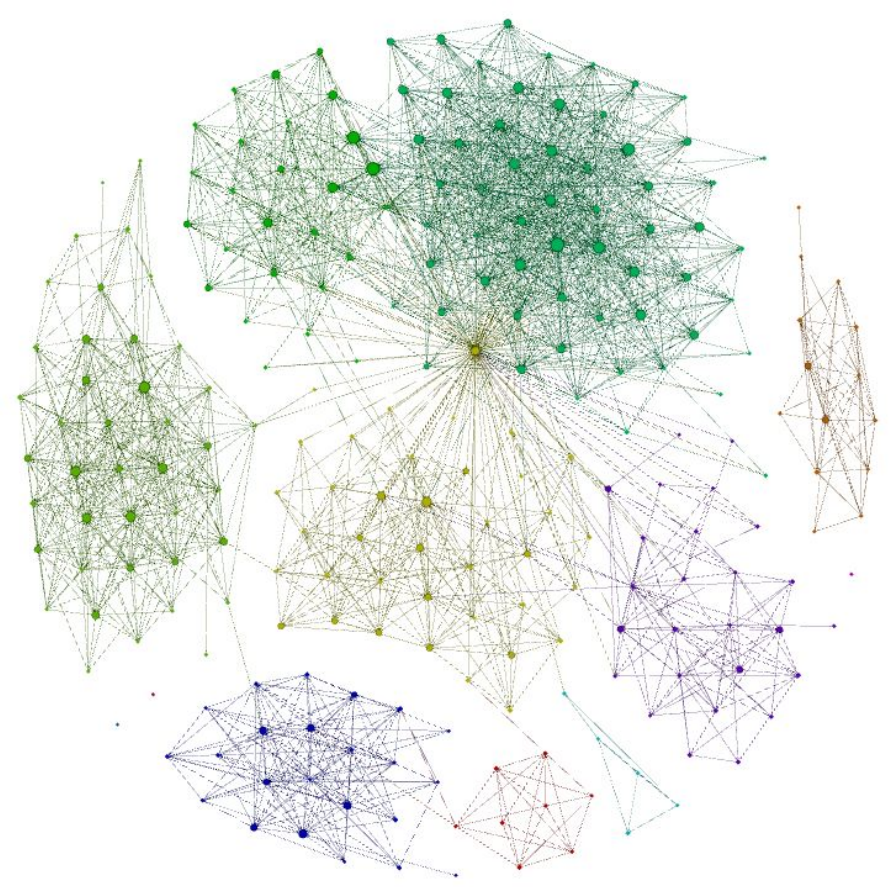
Applications



Shamir, Rivest and Adleman

- Password management
- **Commitment schemes**
  - Coin flipping over the phone?!
- Digital signatures
- **Public-key cryptography**: the RSA method and relatives

A public-key cryptosystem based on graphs



- What are graphs?
- How can we code a number using a graph?
- How to decode?
- Complexity and speed of calculations

A friendship network from Facebook
(http://allthingsgraphed.com)

What would you like to know now?

Thanks!