

# Cryptography and Beyond..

Csaba Szepesvári

Lunch and Learn Seminar

szepesva@cs...

Department of Computing Science

University of Alberta

July 29, 2009

Slides at: [www.cs.ualberta.ca/~szepesva/crypto/](http://www.cs.ualberta.ca/~szepesva/crypto/)

# Contents

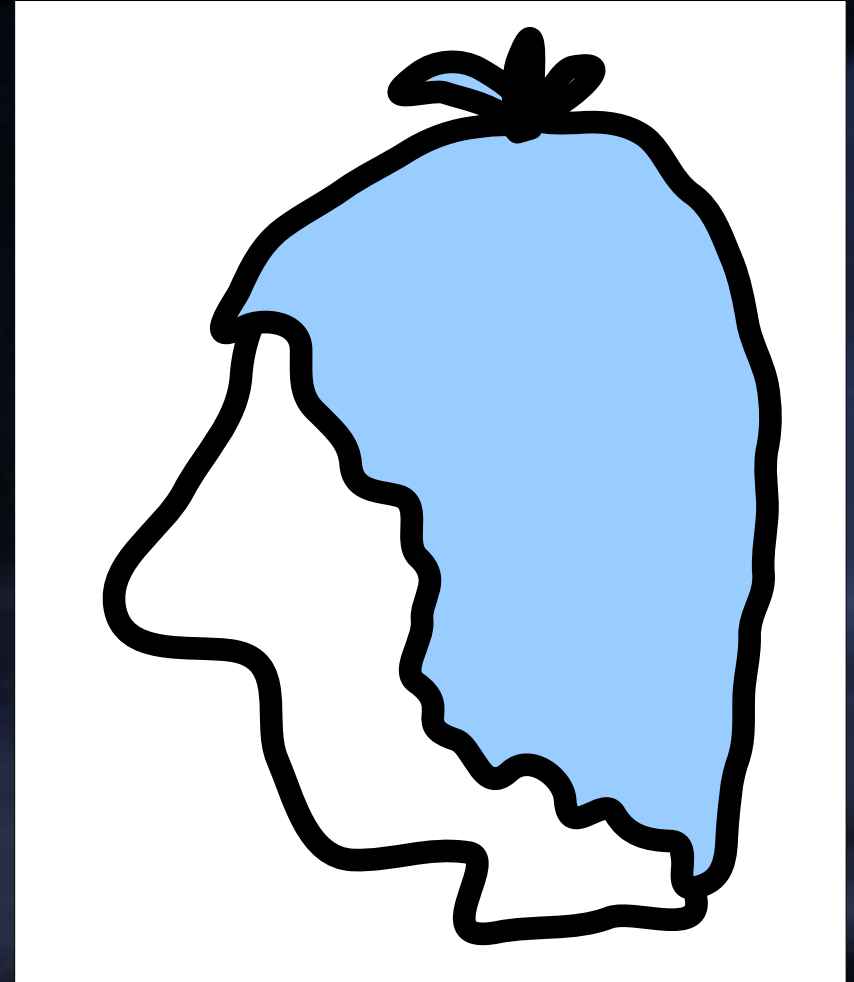
4000 BCE	<b>4000 years before...</b>
500 BCE	<b>The Spartans and Romans</b>
1000	<b>Frequency Analysis</b>
1467	<b>Cipher Disk</b>
1523	<b>Vigenère</b>
1799	<b>Light Experiments</b>
1918	<b>Enigma</b>
1949	<b>Shannon</b>
1970	<b>Quantum Money</b>
1973	<b>Horst Feistel</b>
1975	<b>Public Key Cryptography</b>
1976	<b>Diffie-Hellman- Merkel</b>
1977	<b>DES RSA</b>
1979	<b>ATM using DES</b>
1982	<b>R. Feynman</b>
1984	<b>BB84</b>
1994	<b>Peter Shor</b>
1997	<b>DES Challenge</b>
1998	<b>Quantum Computing</b>
2001	<b>AES</b>

- Ancient methods
- Middle ages
- Modern technology
- Zero-knowledge proofs and all that..

# The Beginning: Ancient Tricks



- Wax tablet



# Ancient Methods

- Skytale (AD 600)
- transposition cipher:



(1,2)
(3,4)
(2,3)

- Ceaser's cipher:

CAESAR =>FDHVDU

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
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

- monoalphabetic substitution cipher

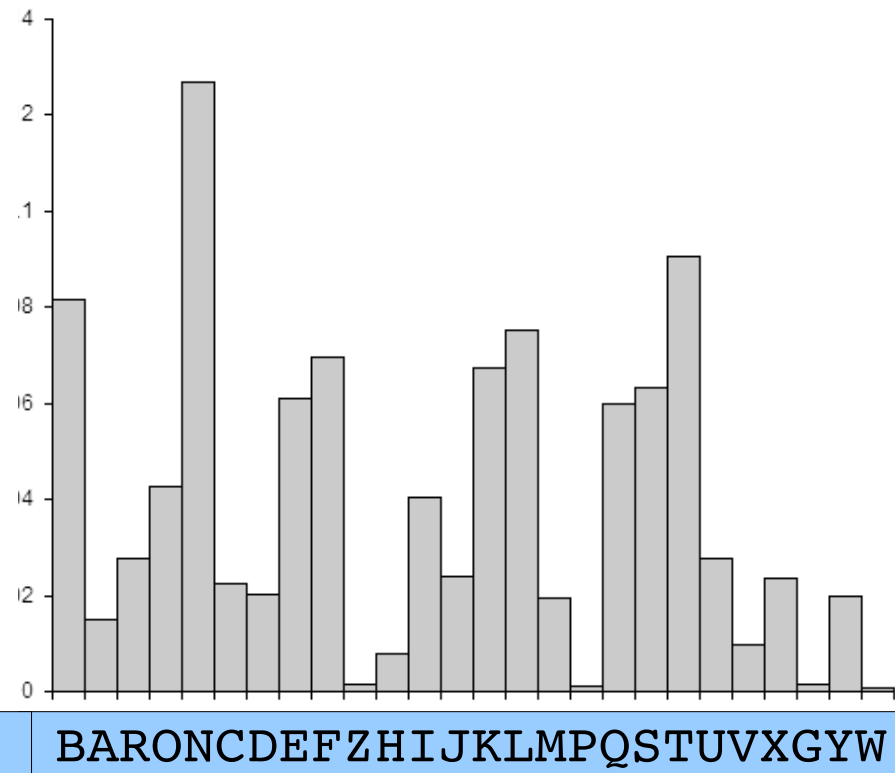
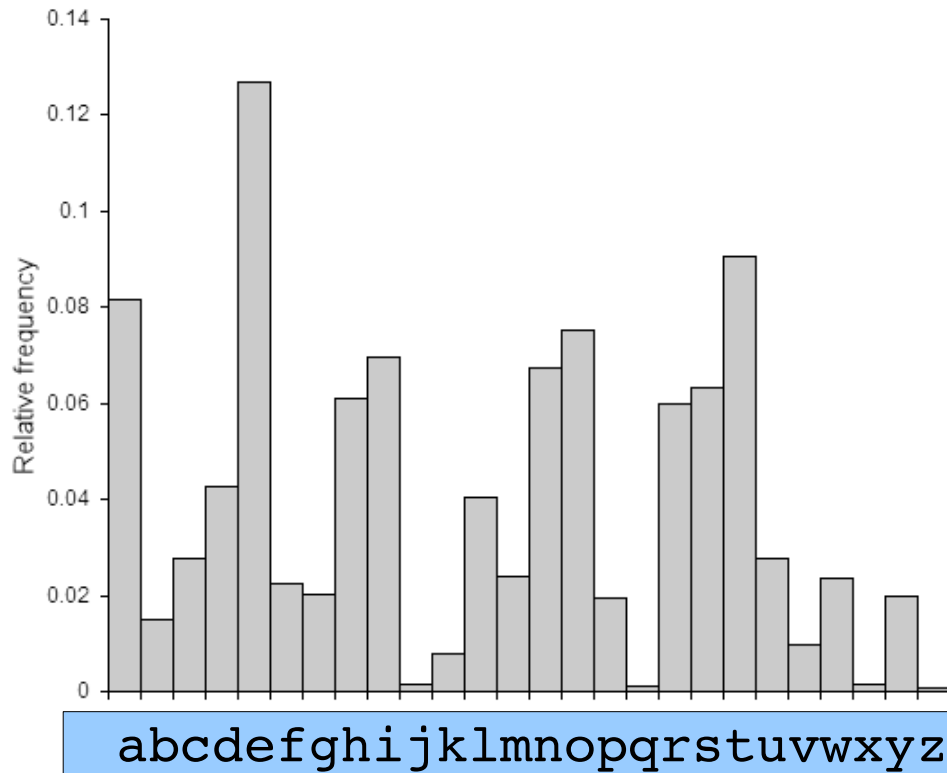
# Breaking monoalphabetic substitution codes

abcdefghijklmnopqrstuvwxyz  
BARONCDEFZHIJKLMPQSTUVXGYW

- Number of codes is enormous!
  - 26! is ca.  
10 000 000 000 000 000 000 000 000 000 000 000
- 9th century,
- Abū-Yūsuf Ya'qūb ibn Ishāq al-Kindī
- 290 books, one book about cryptography!
- How could he solve it???

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

# The frequency method



# Illustration

## FREQUENCIES(%)

Message English

L: 10.3 e: 12.7

K: 9.7 t: 9.1

T: 9.7 a: 8.2

F: 8.0 i: 7.0

N: 7.6 n: 6.7

B: 6.2 o: 6.3

Q: 6.2 h: 6.1

S: 6.2 r: 6.0

R: 5.5 d: 4.3

C: 4.8 q: 4.3

E: 4.8 l: 4.0

M: 3.4 c: 2.8

U: 3.4 u: 2.8

NKDIF SERLJ MIBFK FKDLV  
 NQIBR HLCJU KFTFL KSTEN  
 YQNDQ NTTEB TTENM QLJFS  
 NOSUM MLQTL CTENC QNKRE  
 BTTBR HKLQT ELCBQ QBSFS  
 KLTML SSFAI NLKBR RLUKT  
 LCJUK FTFLK FKSUC CFRFN  
 KRYXB

Message from the most successful German spy in the First World War; Baron August Schluga (Agent 17) - ciphertext

Message: TE, FK, BR, LC, EN, TT, NK, KD, RL, LJ

English: th, he, in, er, ed, an, nd, ar, re, en

# The solution..

en i h o in in o e o nitio n the e etth tthe o i  
NKDIF SERLJ MIBFK FKDLV NQIBR HLCJU KFTFL KSTEN YONDQ NTTEB TTENM QLJFS  
e o to the en h tt no t ho i not o i eon o nt  
NOSUM MLQTL CTENC QNKRE BTTBR HKLQT ELCBQ QBSFS KLTML SSFAI NLKBR RLUKT  
o n ition in i ie n  
LCJUK FTFLK FKSUC CFRFN KRYXB

engli shcom plain ingov erlac kofmu nitio nsthe yregr ettha tthep romis  
edsup porto fthef rench attac knort hofar rasis notpo ssibl eonac count  
ofmun ition insuf ficie ncywa

english complaining over lack of munitions  
they regret that the promised support of the french attack north of  
arras is not possible on account of munition insufficiency  
wa

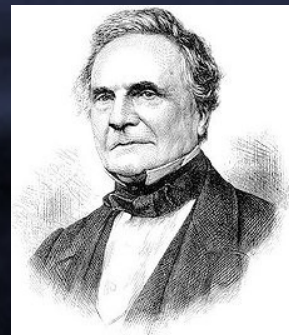


Solve it on your own!

Automated Solver

# Improved encryption in the middle ages

- The Alberti Cipher Disk (15<sup>th</sup> century)
- Vigenère (16<sup>th</sup> century)
  - Change the substitution code character to character
  - “polyalphabetic” cipher
  - $C_i \equiv P_i + K_i \pmod{26}$
- The “Unbreakable Cipher”
- Too complicated, broken by Babbage



Babbage (ca. 1860)

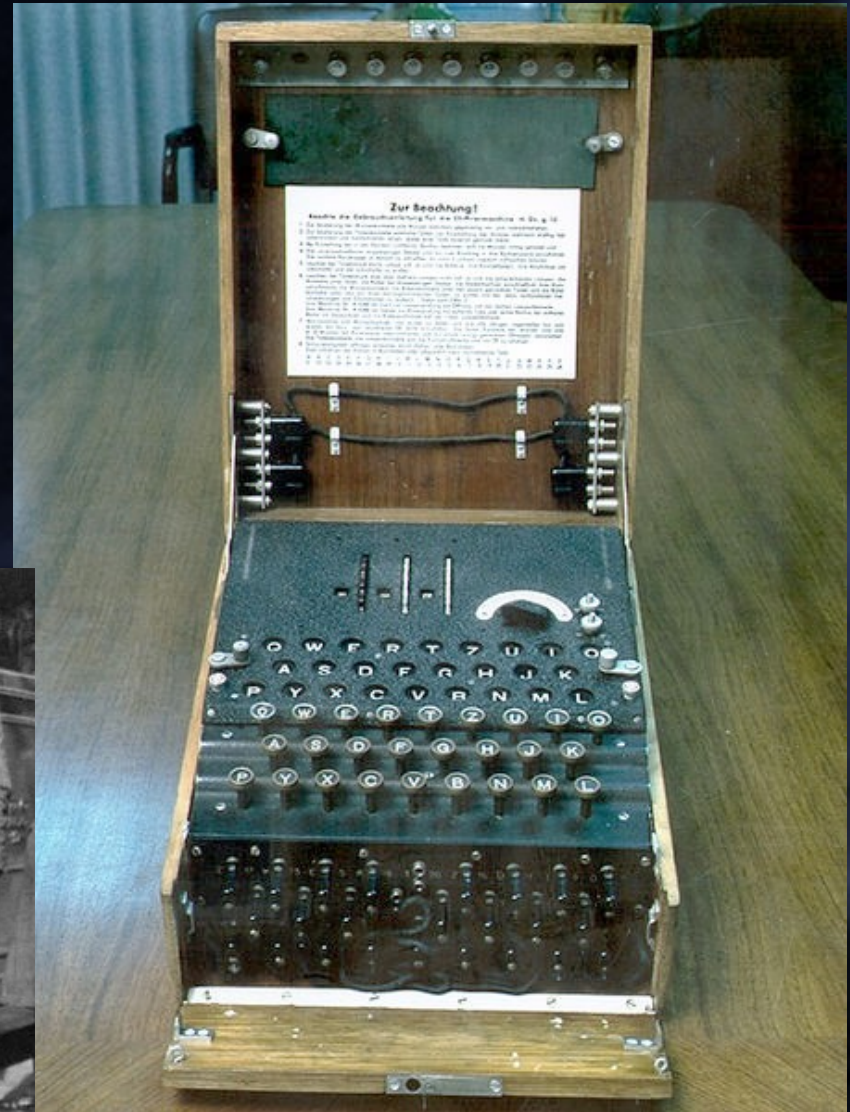
# Weaknesses and strengths

- Key property used in analysis:  
In English the frequency of characters, character-pairs, .. is non-uniform

	<b>Weakness</b>	<b>Strength</b>
<b>Transposition</b>	Keeps letters	Mixes neighbors “diffusion”
<b>Substitution</b>	Keeps neighbors	Mixes letters “confusion”

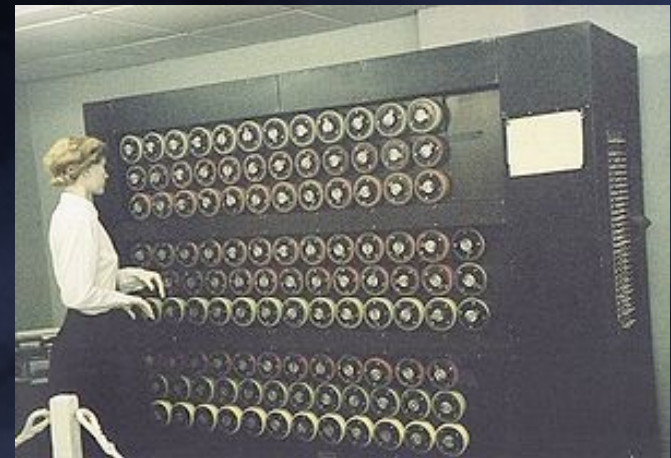
# Modern era: 2<sup>nd</sup> World War

- Enigma
  - Substitution
  - Transposition
- Rejewski, Newman, Turing



# How could they break Enigma?

- The encryption method became known – just the “keys” were unknown
- Keys were sometimes caught, repeated,..
- Cribs were discovered (“eins” was used in 90% of the text)
- Enigma had cryptographic weaknesses
- Higher math, automation
- .. still, success rate varied a lot!



# The Age of Modern Communication



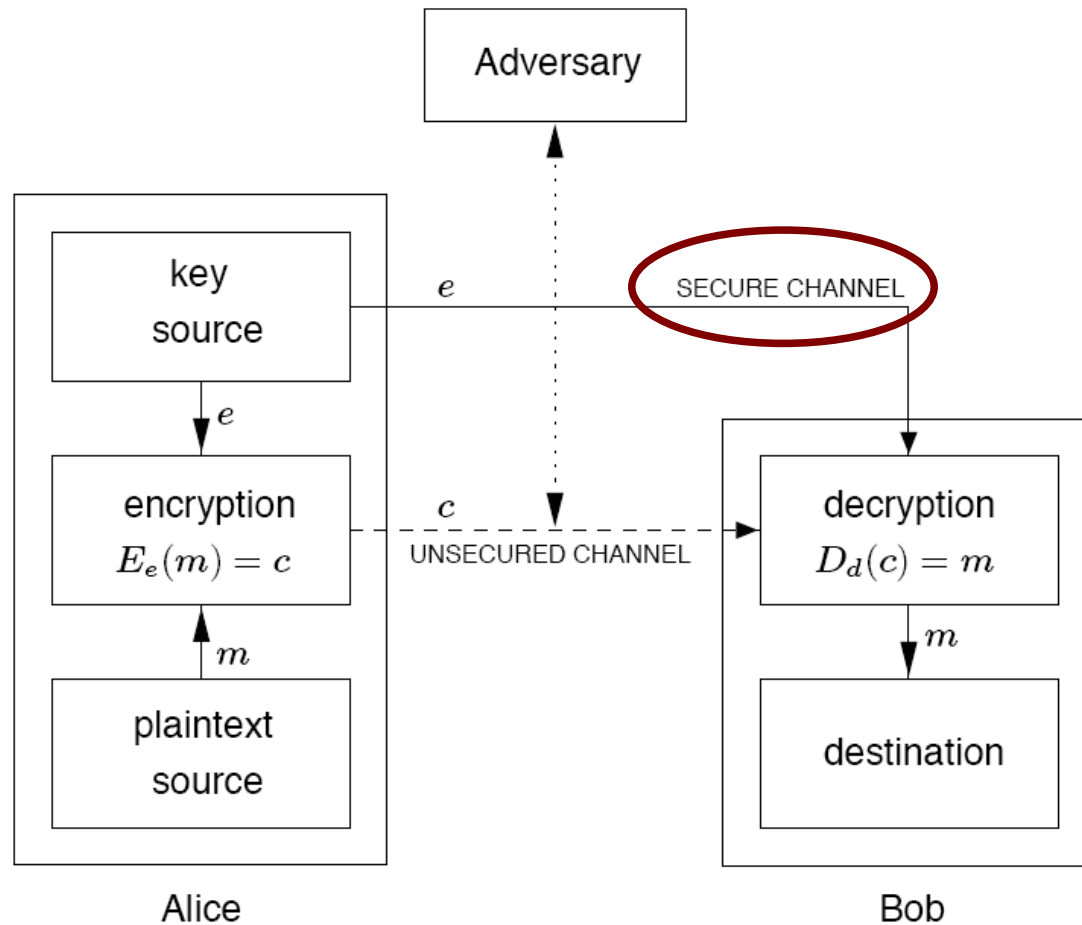
- Radio, telephone, internet:  
*insecure communication lines!*
- Keys need to be changed frequently
- What if a “codebook” is caught?
  - Code is broken!
  - Impersonation!
- How to send new keys??
- ==> KEY DISTRIBUTION PROBLEM

# How does cryptography work?

## **Kerckhoffs' (1883) desiderata**

- i. the system should be, if not theoretically unbreakable, unbreakable in practice;
- ii. compromise of the system details should not inconvenience the correspondents;
- iii. the key should be rememberable without notes and easily changed;
- iv. the cryptogram should be transmissible by telegraph;
- v. the encryption apparatus should be portable and operable by a single person; and
- vi. the system should be easy, requiring neither the knowledge of a long list of rules nor mental strain.

# How does cryptography work?



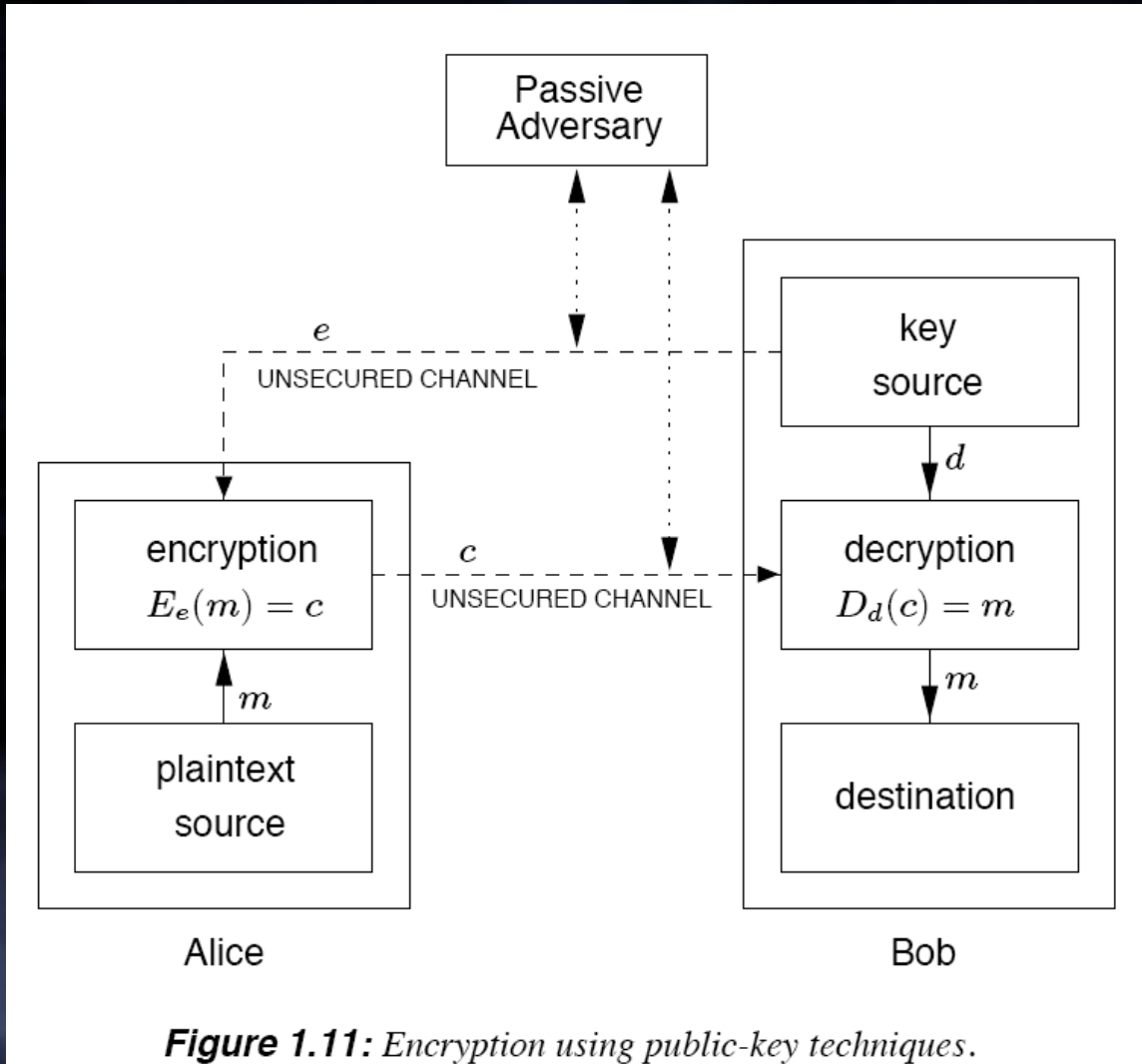
**Figure 1.7:** Two-party communication using encryption, with a secure channel for key exchange. The decryption key  $d$  can be efficiently computed from the encryption key  $e$ .

# How can keys be distributed in a secure and cheap manner?

- Cost matters!
- Speed matters!



# Public key cryptography

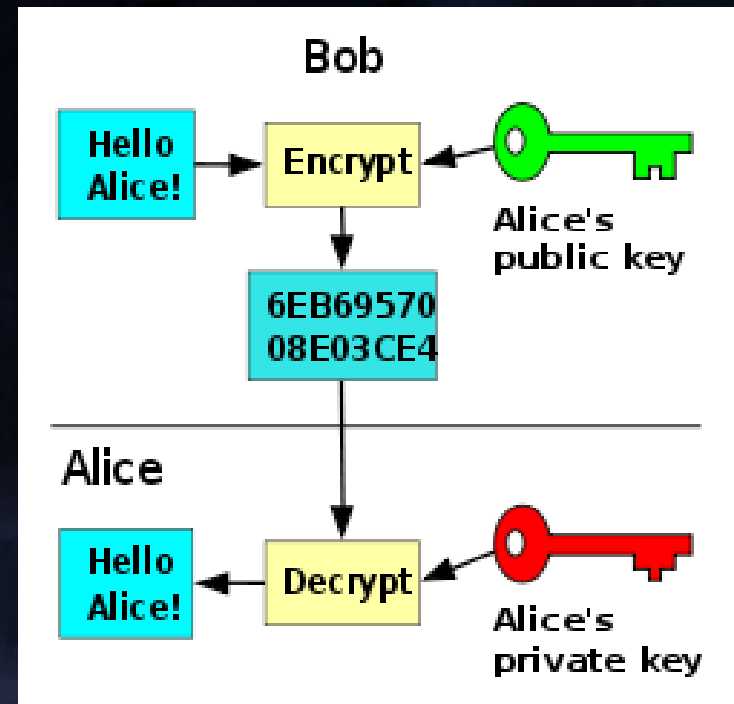
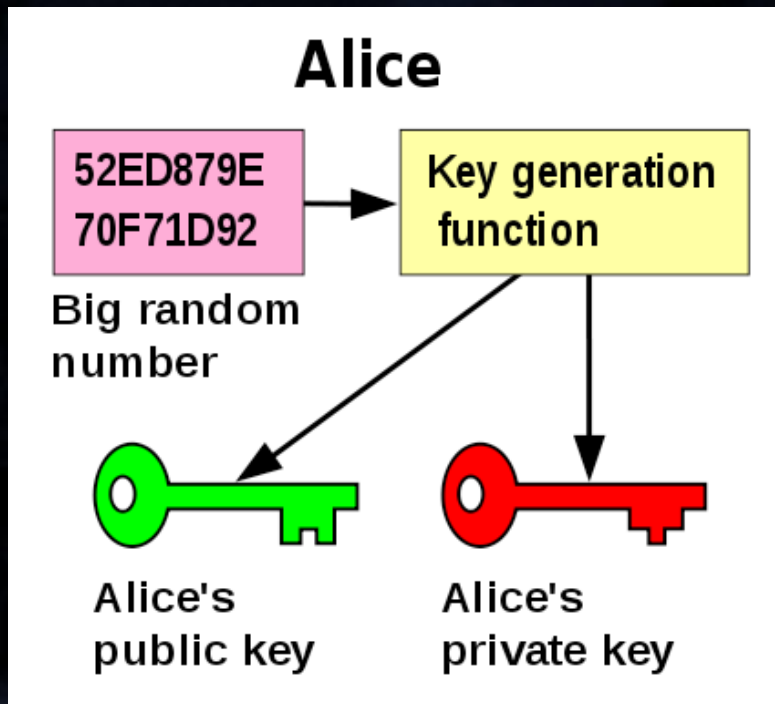


**Figure 1.11:** Encryption using public-key techniques.

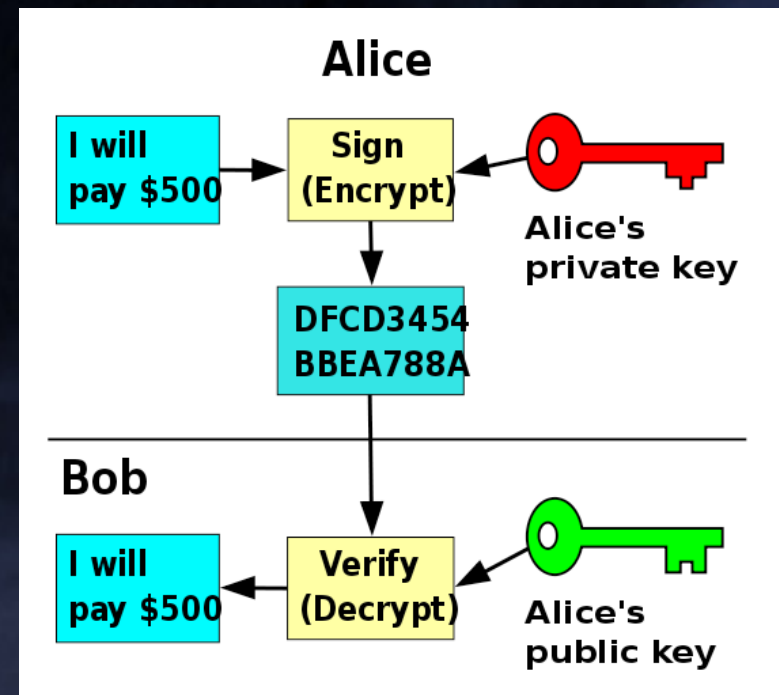
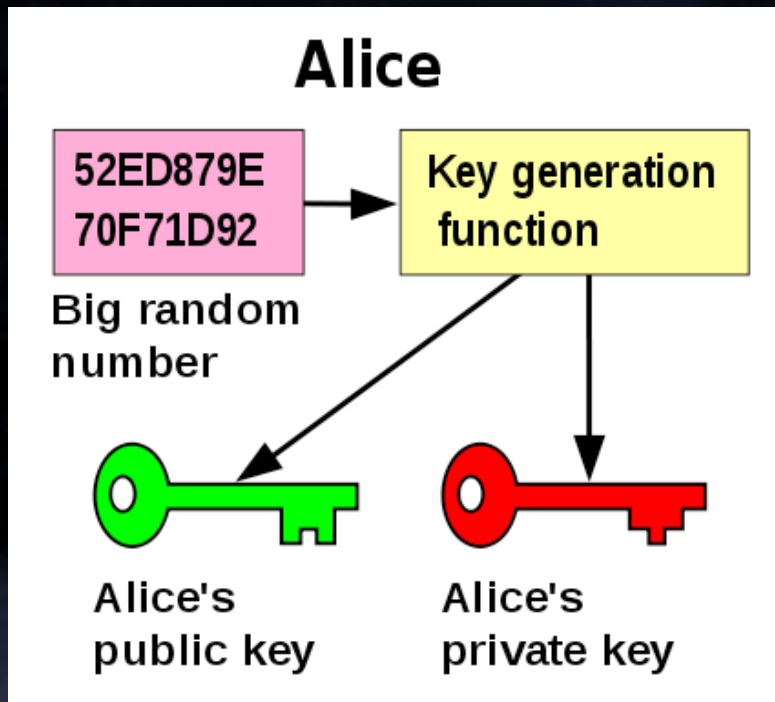


Diffie-Hellman (1976) -Merkle (1974) – Ellis (1969), Crock (1973), Williamson (1974)

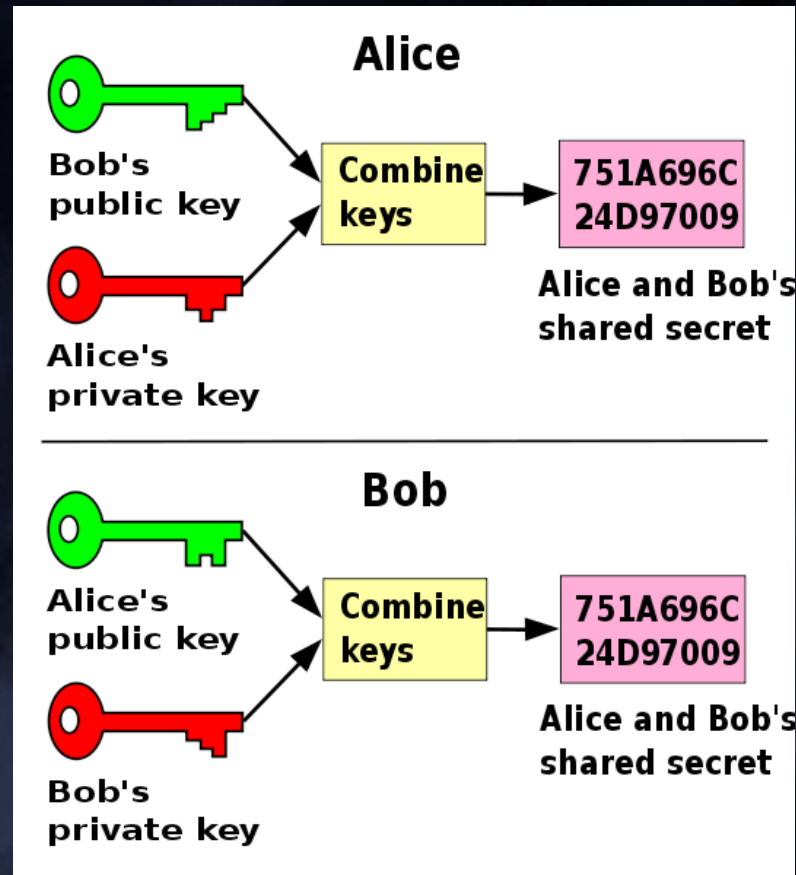
# Public-key cryptography



# Digital signatures



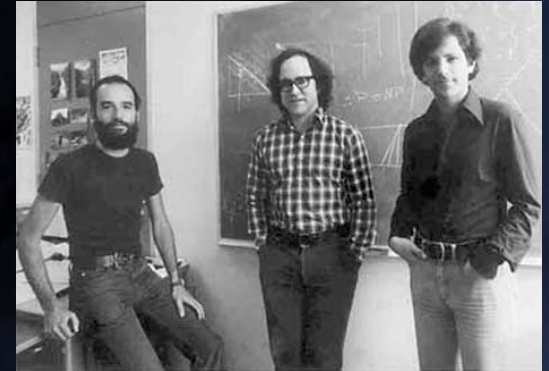
# Public-key cryptography: generating secret shared keys



Diffie-Hellman key exchange

# An implementation: Rivest-Shamir-Adleman coding

- Key generation
  - Choose  $p, q$  primes,  $n = pq$
  - Choose  $1 < e < \phi(n)$ ,  $e, \phi(n)$  coprime
  - Find  $d$  st.  $de \equiv 1 \pmod{\phi(n)}$
- Encryption
  - Given  $0 < m < n$ , compute  $c \equiv m^e \pmod{n}$
- Decryption
  - Given  $c$ , recover  $m$  using  $m \equiv c^d \pmod{n}$



(1978)



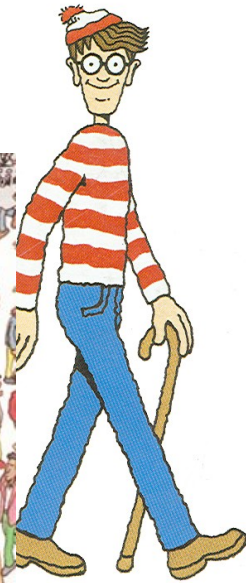
# Goals of cryptography

- Confidentiality (or secrecy)
  - Outsiders should not access the information in the message
- Data integrity
  - Prevent unauthorized change of data
- Authentication
  - Parties should authenticate
  - Information origin, date of origin, data content should be authenticated
- Non-repudiation
  - No way of denying that certain actions were taken

# Zero-knowledge proof systems

- Problem: Prove that you know a secret without telling it!
- Examples:
  - Selling an idea that solves a famous problem!
  - Password authentication
  - Enforce honest behavior while maintaining privacy:
    - Secret: how the user behaves

# Where is Waldo?



(Naor, Naor, Reingold, 1999)

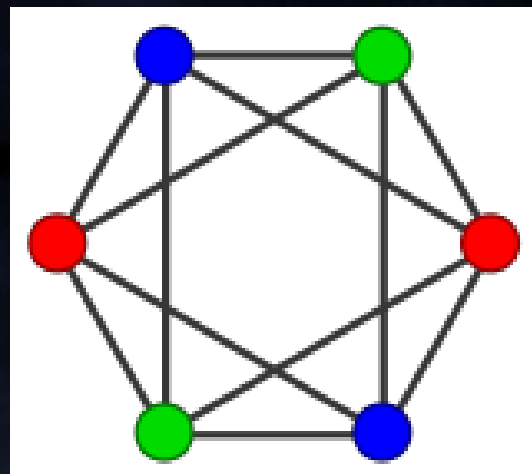
# Flipping a coin over the phone

- Problem: Flip a coin over the phone, avoid disputes!
- Alice:
  - Choose large primes  $p, q$ , st.  $p, q \equiv i \pmod{4}$ , where  $i \in \{1, 3\}$
  - Tell  $n = pq$  Bob.
- Bob:
  - Call  $j \in \{1, 3\}$
- Winner:
  - Bob if  $p, q \equiv j \pmod{4}$ , otherwise Alice.

Fair?  
No disputes?

# 3-coloring of graphs

- Secret: The 3-coloring of a graph



- Send solutions to me!
- Win a lunch in the Faculty Club!
- Deadline: A week from now

# Conclusions



- Cryptography is a lot of fun!
- ..because it uses..
  - Nice math (number theory and more)
  - Computer science (what can be computed efficiently)
  - Statistics (exploiting patterns)
  - ...
- Think out of the box!



# The math of RSA: Number theory

## Fermat's Little Theorem (1640)

Let  $p$  be a prime,  $a$  be a natural number. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Proof:** By induction, using the elementary identity

$$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

**Euler's Theorem (1736):** Let  $a$  and  $n$  be coprimes. Let

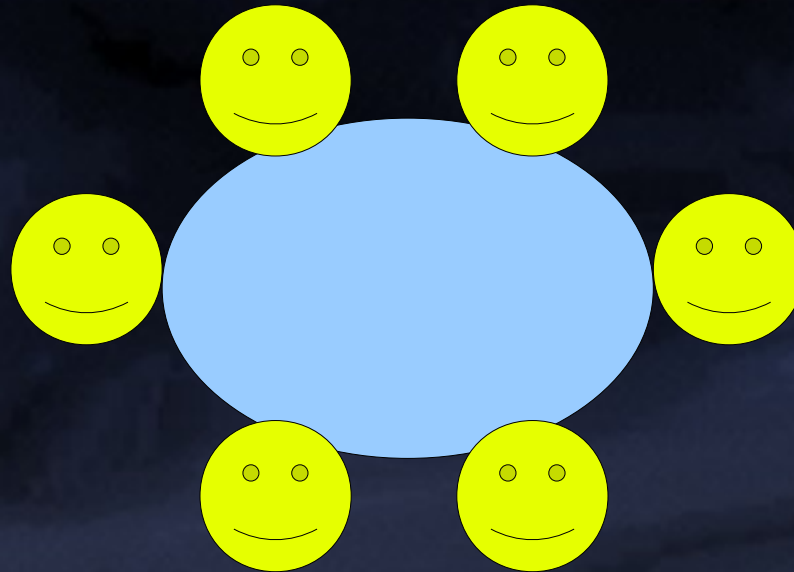
$$\phi(n) = |\{1 \leq i \leq n \mid i \text{ and } n \text{ are coprimes}\}|.$$

Then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

# Dining Cryptographers

- Problem: How to share your secret while staying anonymous?



Who payed the bill?

# Solution

Let  $n$  be the number of cryptographers.

Let  $s_i = 1$  denote if cryptographer  $i$  payed,  $s_i = 0$  otherwise.

(Note:  $s_i = 1$  for exactly one  $i$ .)

Each pair of cryptographers secretly flips a coin.

Let the results be  $b_{ij} \in \{0, 1\}$ .

Cryptographer  $i$  computes

$$c_i = s_i \oplus \left( \bigoplus_{j \neq i} b_{ij} \right),$$

which she/he announces.

Everyone computes

$$c = \bigoplus_{i=1}^n c_i.$$

**Claim:**  $c = \sum_i s_i$ .