Introduction to Cryptography

Ara Balaki

University of Ostrava

28th of Feb. 2023

Cryptography

Secret Writing

“Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behaviour”

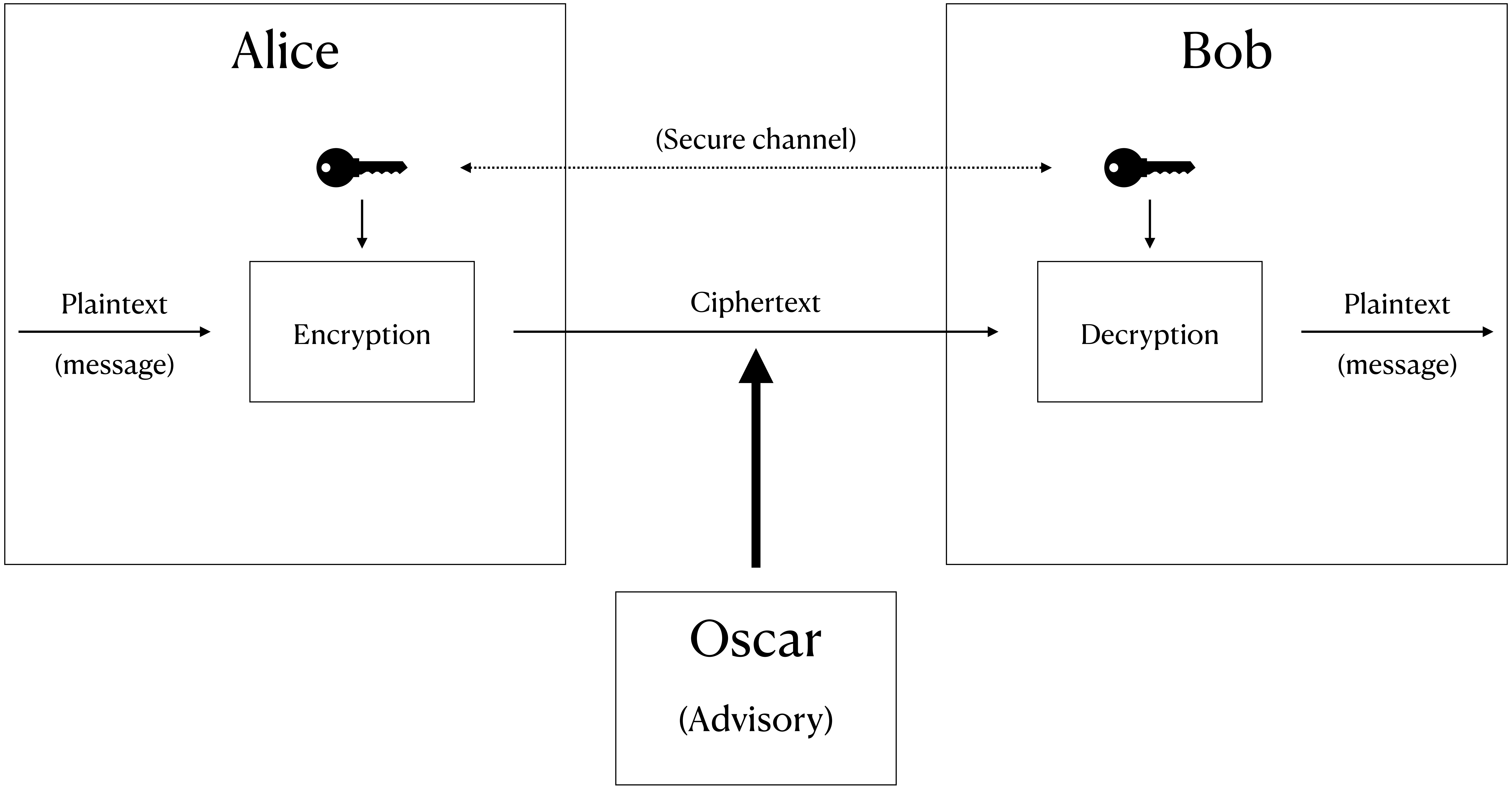
Ronald Linn Rivest

What is Cryptography?

- To enable **secure** communication between two parties. Usually in the literature the parties involved are denoted by **Alice** and **Bob**, and the advisory by **Oscar**.
- The process of hiding **messages** (**plaintext**) is called **Encryption** and the process of revealing hidden messages is **Decryption**.
- A **Cipher** is the algorithm for preforming encryption and decryption; the plaintext that has been through a encryption cipher is called **ciphertext**.
- To make ciphers not predictable, the process is varied using a **key**, prior to encryption a key must be selected.
- Without the knowledge of the key, decryption should <u>very hard</u>, if not impossible.

What is Cryptography?

General Model



Now that we have an idea of what cryptography is, the question now is...

How to do Cryptography?

Classical Ciphers

Caesar Cipher

- To encrypt, each letter of the plaintext is substituted by a letter three places down the alphabet.
- It is a **substitution** cipher.
- Allegedly used by Julies Caesar.

Caesar Cipher

Mathematical interpretation

- We can interpret the Caeser cipher by shifting alphabet by three places.

Plain	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
Cipher	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

- If we map each letter to positions value in the alphabet, then let M_i be the i^{th} letter of the message then we can define the encryption and decryption the following way

$$E(M_i) = M_i + 3 \mod 26$$

$$D(M_i) = M_i - 3 \mod 26$$

Caesar Cipher

Mathematical interpretation

- Of course there is nothing special about shifting the letters by three, in general we could use any $k \in \{0,1, \dots ,25\}$

$$E_k(M_i) = M_i + k \mod 26$$

$$D_k(C_i) = C_i - k \mod 26$$

- Here k **key** of cipher and the set $\{0,1, \dots ,25\}$ is the **key space**.
- Examples.

$$\texttt{ATTACKNOW} \rightarrow \texttt{DWWDFNQRZ}$$

$$\texttt{SENDREINFORCEMENTS} \rightarrow \texttt{PBKAOBFKCLOZBJBKQP}$$

Caesar Cipher

Cryptanalysis

- A cryptographic **attack** is a method that attempts to decrypt a ciphertext without full (or partial) knowledge of the key, by weakness in the **crypto-system**.
- It is trivially easy to break the Caesars cipher for a cryptanalyst.
- First, because of it's small key space, a simple **brute force** attack such as a key-search would be able to reveal ciphertext in a very short period of time.
- Another weakness in this cipher is that the frequency of the letters will not change, and so it's susceptible to **Frequency analysis** attacks.

Vigenère cipher

- Much more secure cipher.
- Build from a collection of Caesar ciphers in series.
- Uses a **Tabula Recta**.
- The key is a repeated keyword.
- Thought to be unbreakable.

◉ Originally conceived by *Giovan Battista Bellaso* in 1553, but in the 19th century was wrongly attributed to *Blaise de Vigenère*.

Vigenère cipher

Mathematical interpretation

- It can also be described algebraically, given K_i the i^{th} letter of the key

$$E_k(M_i) = M_i + K_i \mod 26$$

$$D_k(C_i) = C_i - K_i \mod 26$$

- Example.

Given keyword "VICTORY"

Plaintext	ATTACKATDAWN
Key	VICTORYVICTO
Ciphertext	VBVTQBYOLCPB

	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
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Tabula recta

Vigenère cipher

Cryptanalysis

- A key-search attack is unfeasible, as the key space is massive; more precisely a message of length l has 26^l possible keys.
- The Vigenere cipher is an example of polyalphabetic substitution cipher, where it the plaintext's letter frequency disguised.
- It is resistant to straight forward frequency analysis attacks.

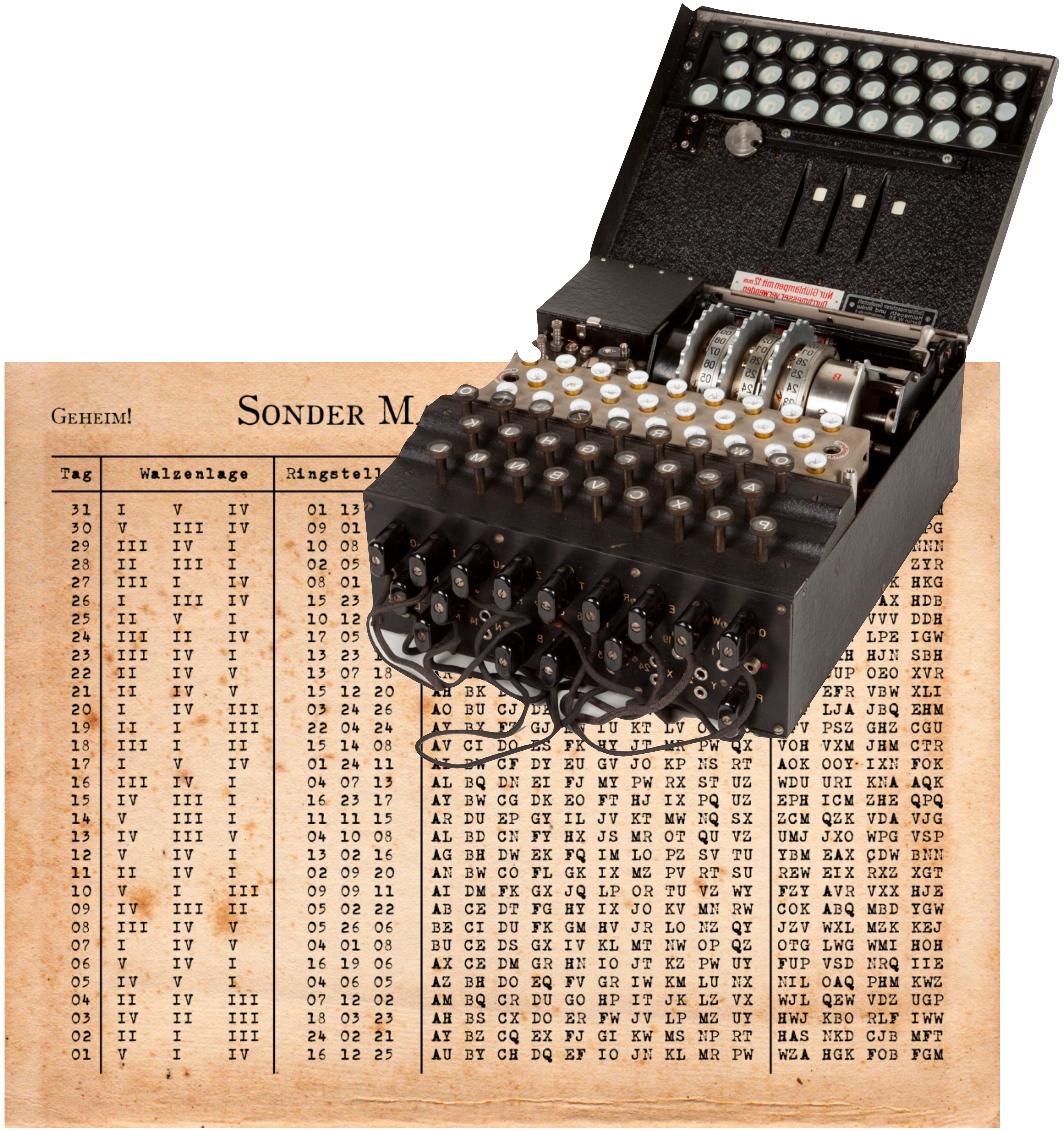
Vigenère cipher

Cryptanalysis

- The great weakness of this cipher lies in the repeating nature of the key.
- If the length of the key is know *n*, then the cryptanalysis is of *n* Caeser ciphers, that can be broken individually.
- There are many methods to guess the keyword length, namely *Kasiski examination* and *Friedman test*.
- It is known that Charles Babbage in 1854 was the first to developed and break the cipher, but his work was never published.

Enigma

- Rotary based cipher.
- Partly automates ciphering of messages.
- Used by the Germans in the second world war.



Enigma

Cryptanalysis

- In December 1932, Marian Rejewski, polish mathematician and cryptanalyst, was able to break the Enigma cipher by using the theory of permutations.
- Later he and his fellow cryptanalysts continued on improving there methods and invented devices, such as the Bomba, to aid their efforts.
- The poles initiated the British and French military intelligence about the enigma and their decryption techniques and equipment.

Enigma

Cryptanalysis

- During the war British cryptanalysts, most notably in blackly park, decrypted a vast number of messages enciphered on Enigma.
- Most notably the cryptanalysts at Bletchley park, most famous Alan Turning, improved upon the existing methods and were able to break into messages in less then 24 hours.

Modern Cryptography

Modern cryptography

- With the advent of computers, classic ciphers became impractical.
- As the computation power allowed swift and effective attacks against even the strongest of classic pen and paper ciphers.
- Higher standards are required for crypto-systems to be viable.
- So newer methods were developed using computers.

“The Enemy knows the system”

Claude Shannon

Modern cryptography

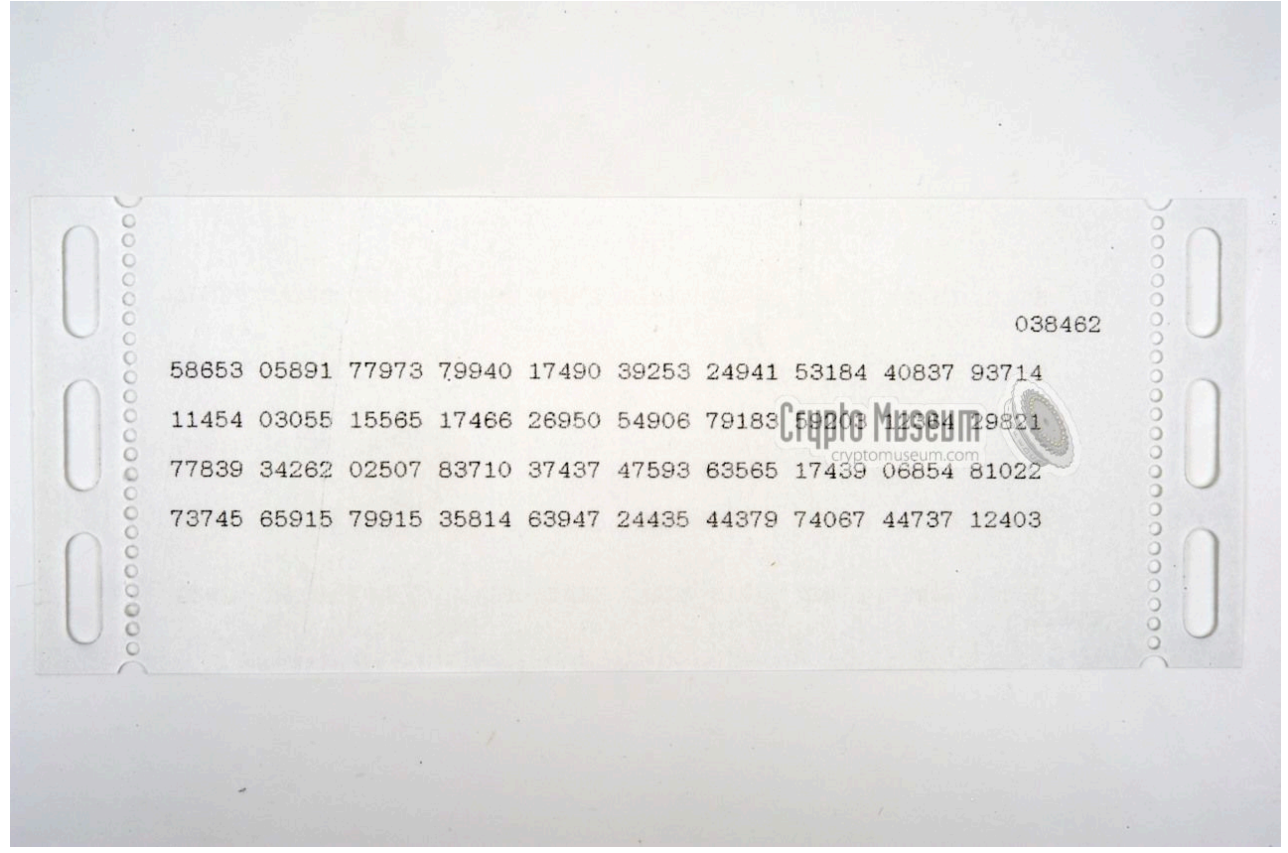
Theoretical beginnings

- In 1948, Claude E. Shannon published the paper *A Mathematical Theory of Communication*, which is seen as the foundation of modern information theory.
- Shannon defined the concept of **perfect secrecy**. A cipher with such a property produces ciphertext that has no statistical relation to the plaintext.
- An example of a cipher with perfect secrecy is **One-time pad**.

One-Time Pad

Unbreakable encryption

- First described by banker Frank Miller in 1882.
- The keys must be truly random.
- And at least the length of the plaintext.
- The function is identical to the simple Vigenère cipher with a infinite and random key.
- Has perfect secrecy.



One-Time Pad

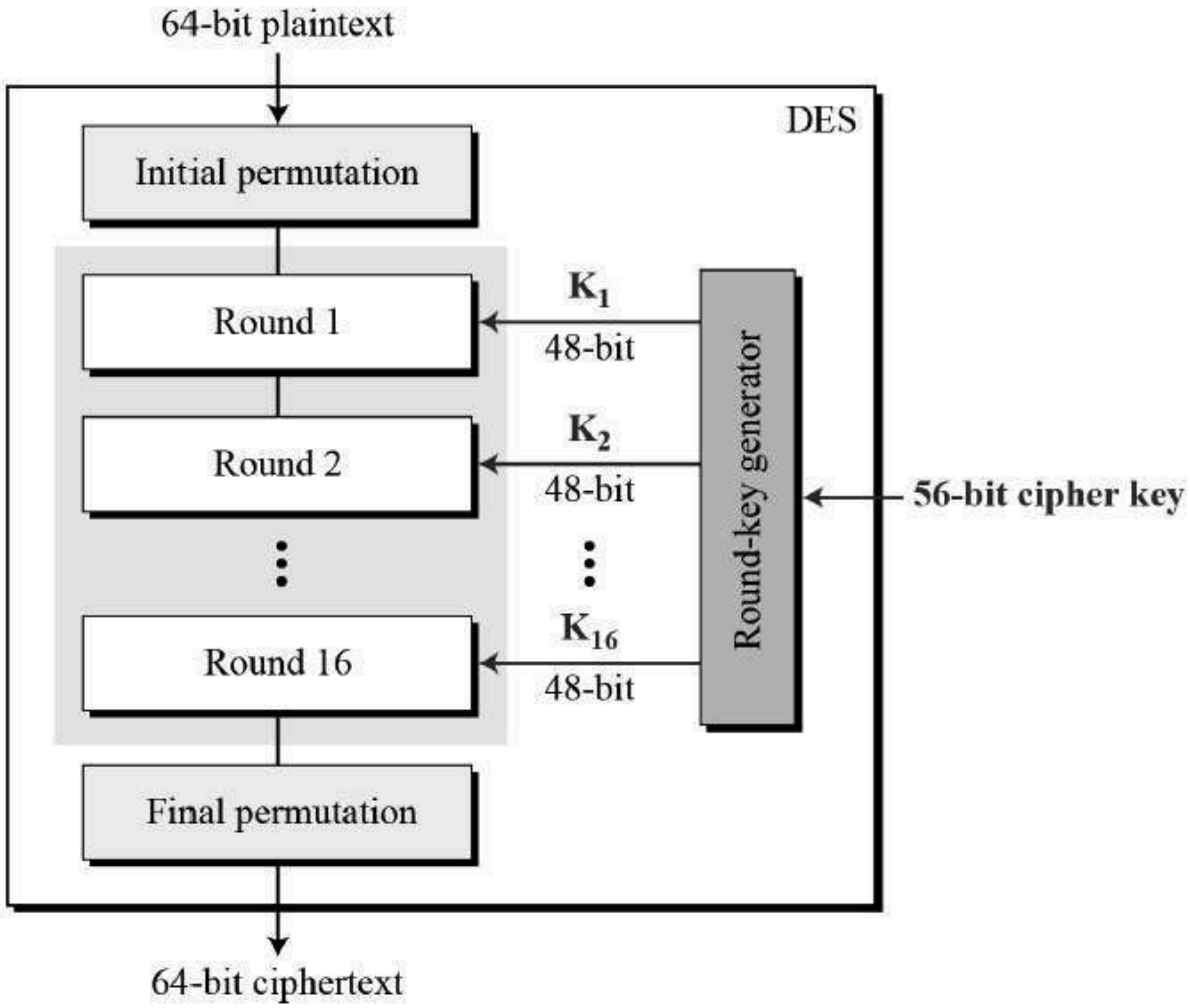
Cryptanalysis

- It is truly unbreakable, if it is properly used.
- It is mathematically proven that any cipher to have perfect secrecy must have the same key requirements.
- The key requirements make it very cumbersome to use.

DES

Data Encryption Standard

- Commissioned by the NSA and developed by IBM in 1972.
- One of the first publicly available modern crypto system that saw wide usage.
- It Is an implementation of a Feistel Cipher.



DES

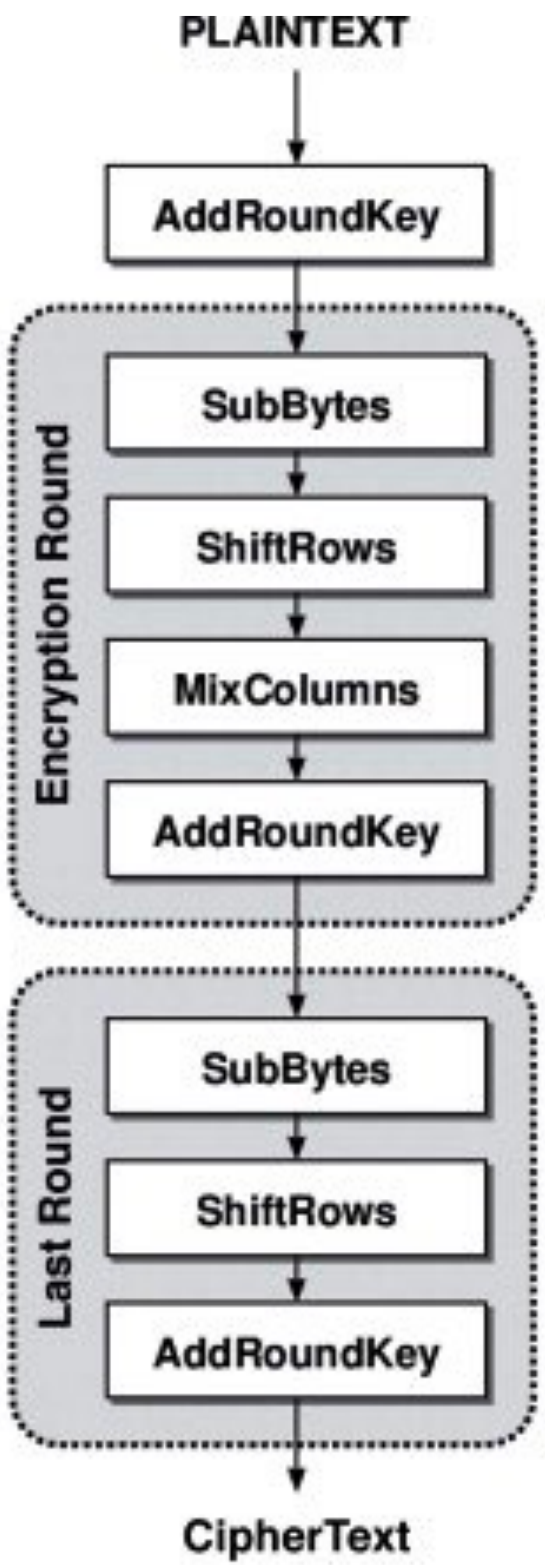
Cryptanalysis

- Although a powerful cipher, many were concerned over its implementation.
- The short key length of 56-bits, and NSAs involvement in the development as such changing the original setting of the S-Boxes.
- Although the suspicions over the weakness of the S-Boxes were relieved, as in 1990 Eli Biham and Adi Shamir independently developed **differential cryptanalysis**, and in a published paper found out that DES S-Boxes are much more resistant then if they were chosen at random.
- In the end the short key size made the cipher insecure against brute force attacks.

AES

AKA Rijndael

- Developed by two Belgian cryptographers,
  Joan Daemen and Vincent Rijmen.
- Originally called Rijndael.
- Proposed to NIST as a replace DES.
- It was accepted as the AES in 2001.



AES

Cryptanalysis

- AES is based on **substitution–permutation network** design.
- It supports key lengths of 128, 192 and 256 bits.
- The calculations are done in the finite field $GF(2)$ with the given irreducible polynomial $x^8 + x^4 + x^3 + x + 1$.
- No practical attacks have been found until now, and it is considered secure for the long term.
- This is by far the most widely used cipher, and it is embedded both into computer software and hardware.

Fundamental issues

- What we have described so far is called **Symmetric-key Cryptography**; Both parties must possess the same key.
- The **key distribution problem** is a fundamental, and the systems in place for solving it can be very complex and error prone.
- So far there is no way to determine that the validity of the messages.

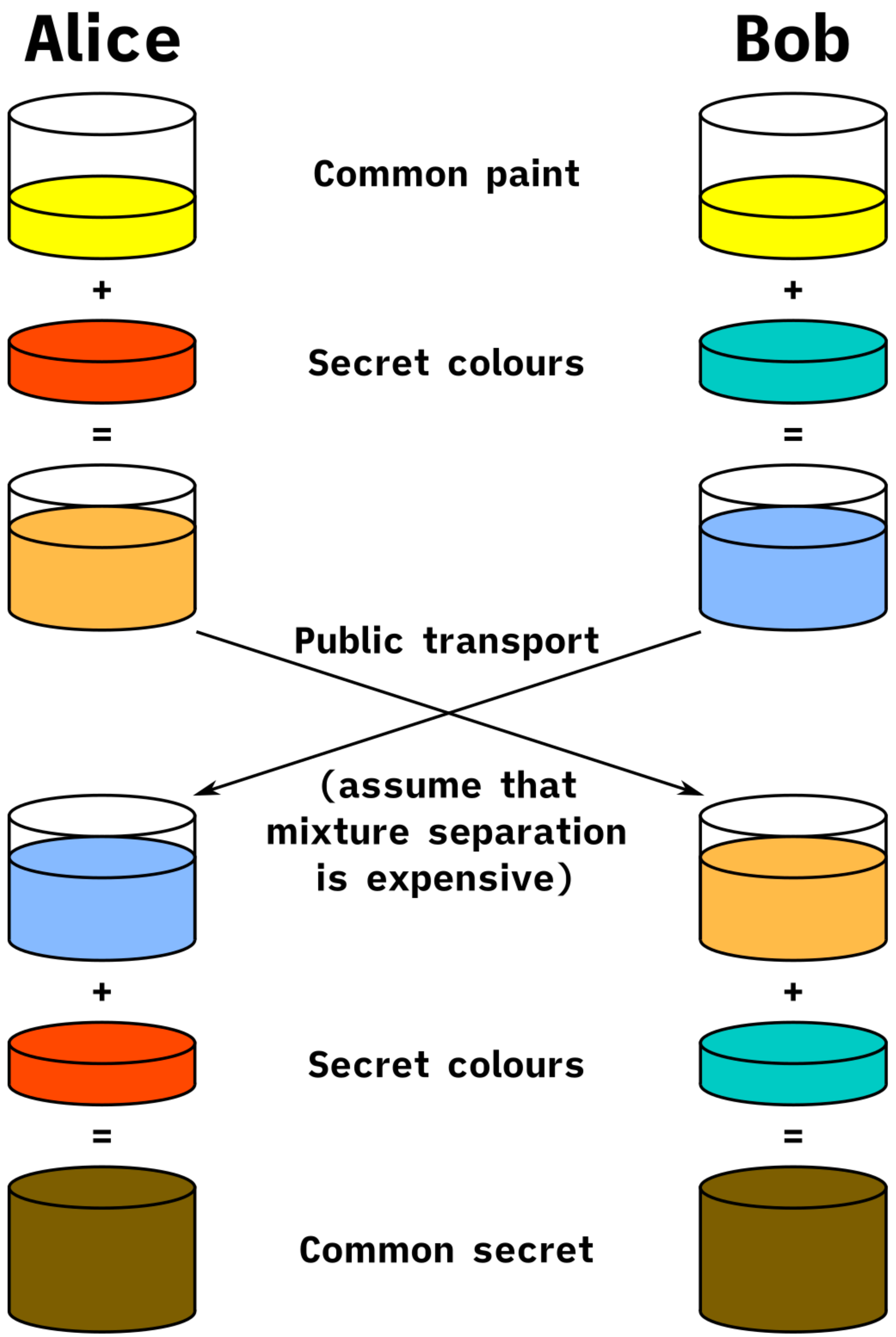
Public-Key Cryptography

Public-Key Cryptography

- Whitfield. Diffie And Martin E. Hellman published *New directions in Cryptography* in the year 1976, in which they proposed a way of doing cryptography.
- In it they proposed public key cryptography.
- Solved both issues of key distribution problem and a proposed way of doing identity validation (**digital signatures**).
- The key idea is to separate encryption and decryption keys to a **public key** and a **private key**.

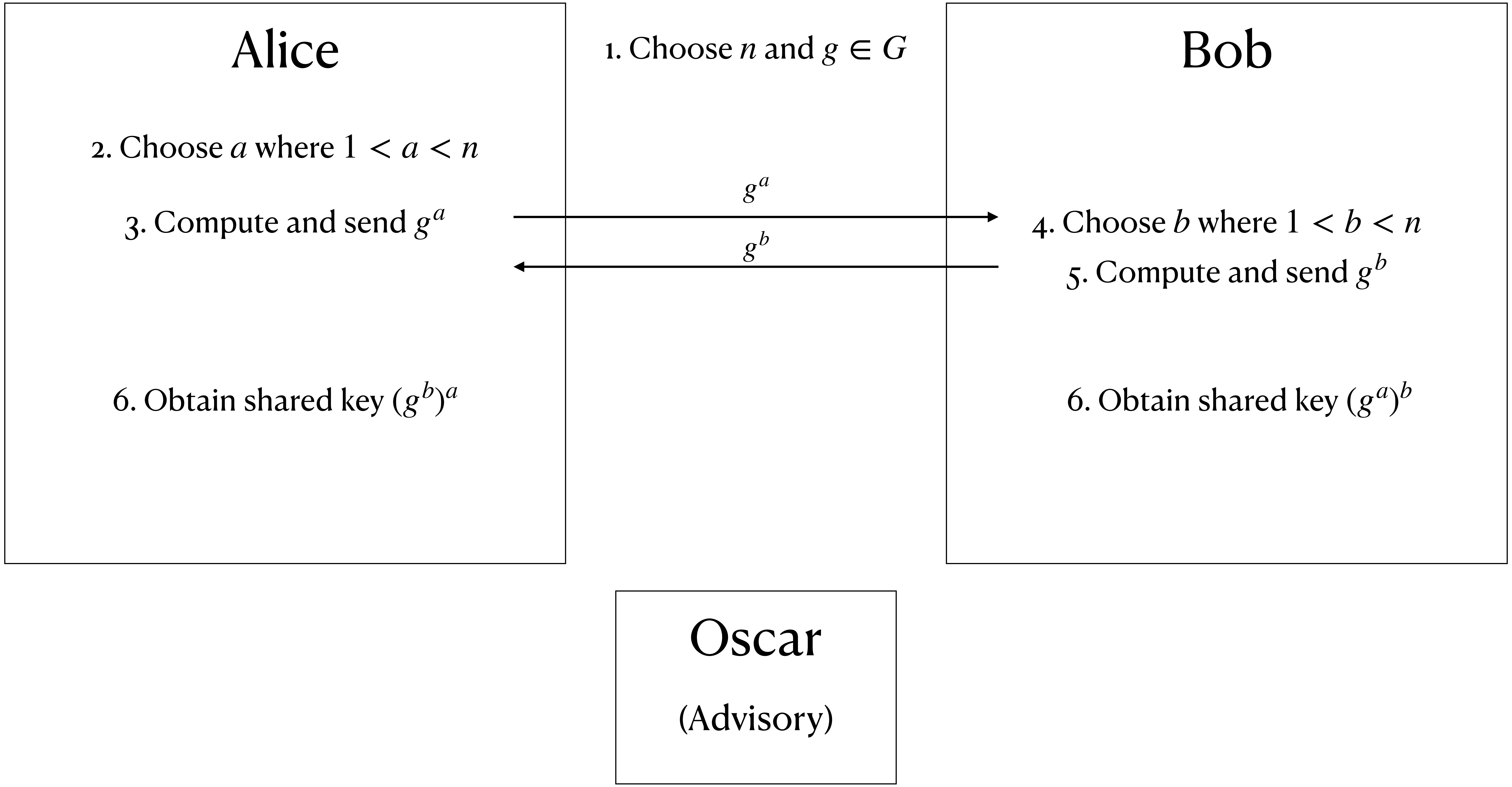
Diffie–Hellman Key Exchange

- First conceived by Ralph Merkle, published in the same paper.
- Solves the key distribution problem.
- Should be paired with symmetric key systems.



Diffie–Hellman Key Exchange

Algorithm



Diffie–Hellman Key Exchange

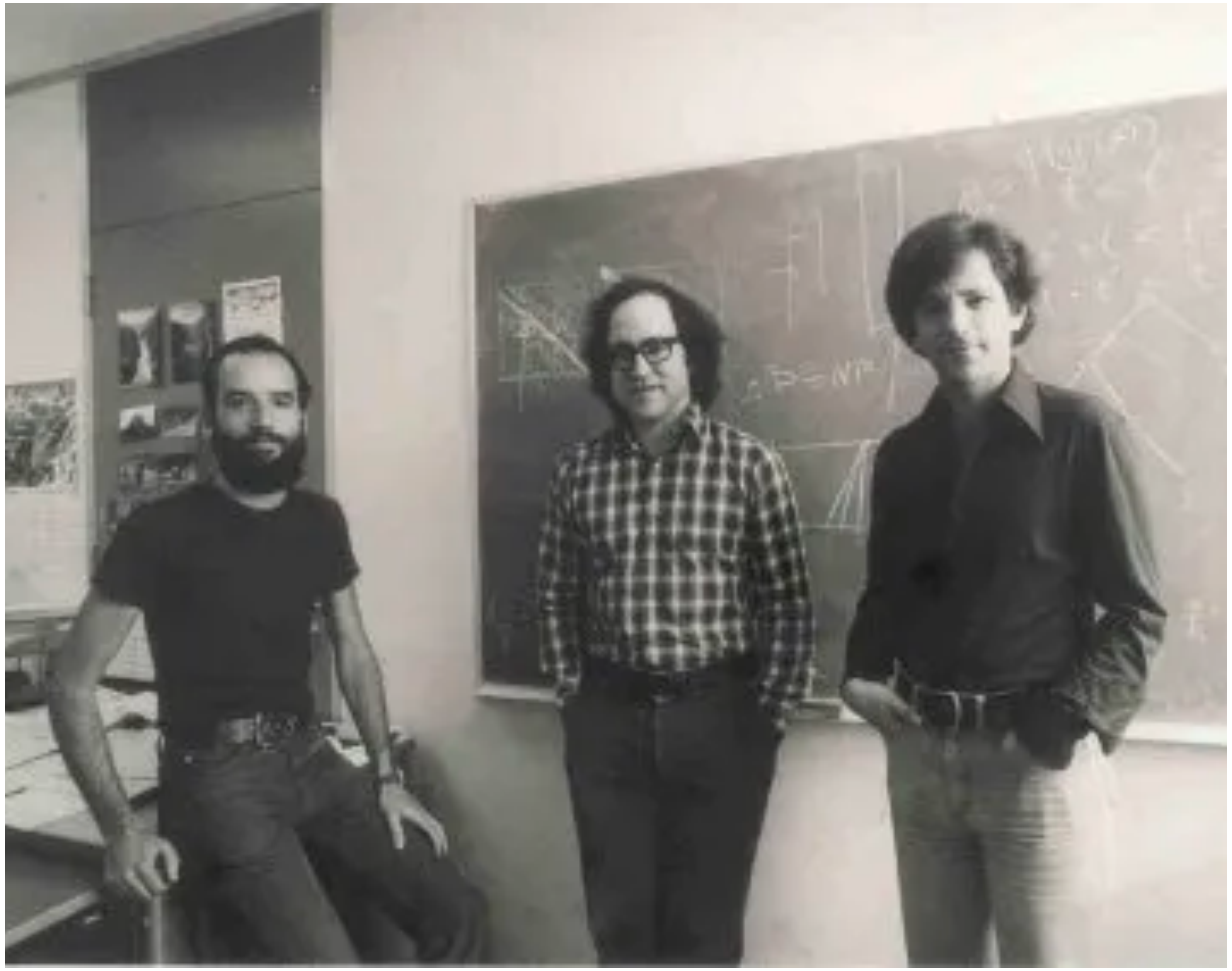
Cryptanalysis

- The security of this crypto-system is based on the fact that even with the knowledge of g^{ab}, g^a, and g^b there is no effective algorithm to compute the private key exponents a or b.
- We can generalise this to the **Discrete Logarithm Problem**. Let G be a cyclic group, and g a generator of G. Given $h \in G$, find the integer t such that $g^t = h$.
- In its most simple form G is multiplicative $\mathbb{Z}_p$ where p is prime.

RSA

Rivest – Shamir – Adleman

- Developed in 1977.
- Uses integer factorisation as its security mechanism.
- Most commonly used public key crypto-system (Web, Banking, etc…)



RSA

Algorithm

- The key generation of RSA

  1. Choose two large primes p and q
  2. Compute $n = pq$
  3. Compute $\phi(n) = (p-1)(q-1)$
  4. Choose e where $2 < e < \phi(n)$ and $\gcd(m, \phi(n)) = 1$
  5. Compute $d \equiv e^{-1} \mod \phi(n)$

The public key is (e, n) and private key d

RSA

Algorithm

- Encryption and decryption are the following operations

$$E(m) = m^e \mod n$$

$$D(c) = c^d = (m^e)^d = m \mod n$$

Notes on group theory in Cryptography

Notes on group theory in Cryptography

- Although number theory is mostly credited for cryptography, but also group theory has played a major role in the development of modern cryptographic system.
- As we saw before we can choose different platform groups for the key exchange protocol, such as group of points on an elliptic curve (elliptic curve cryptography).
- For non-abelian groups **Conjugacy** instead of exponentiation, such as using braid groups in Ko–Lee–Cheon–Han–Kang–Park. Or using the **bracket operator** (**commutator**) in Anshel–Anshel–Goldfeld, for any non-abelian group.
- But so far all of them have major drawbacks and a suitable platform group has yet to be found.

References

- *Understanding Cryptography,* by Christof par.
- *Handbook of Applied Cryptography,* by Alfred Menezes, Paul van Oorschot, and Scott Vanstone.
- *A Mathematical Theory of Communication,* Claude shannon.
- *New Directions in Cryptography*. Whitfield. Diffie And Martin E. Hellman.
- Vist *dcode.fr* for interactive cryptography.

Questions?