Introduction to Cryptography

Vincent Migliore

vincent.migliore@insa-toulouse.fr

INSA-TOULOUSE / LAAS-CNRS

What is cryptography?

Brief introduction to cryptography

INSA TOULOUSE

Definition

Cryptography is the science of *writing* secrets. It is correlated to the evolution of civilizations that are organized as tribes, kingdoms, countries...

Cryptology $\neq$ Cryptography $\neq$ Cryptanalysis

- Cryptology is the science of secret (so a much larger domain than cryptography).
- Cryptanalysis is the science to break secret.

Brief introduction to cryptography

INSA TOULOUSE

Definition

Cryptography is the science of *writing* secrets. It is correlated to the evolution of civilizations that are organized as tribes, kingdoms, countries...

Cryptology $\neq$ Cryptography $\neq$ Cryptanalysis

- Cryptology is the science of secret (so a much larger domain than cryptography).
- Cryptanalysis is the science to break secret.

First known use of cryptography

About 4,000 years ago, Egyptians used hieroglyphs to communicate. Traduction where only known by scribes, civil servants of the monarque, influential persons that are very close to the power.

Question

How hieroglyphs had been decrypted in XIX^e century?

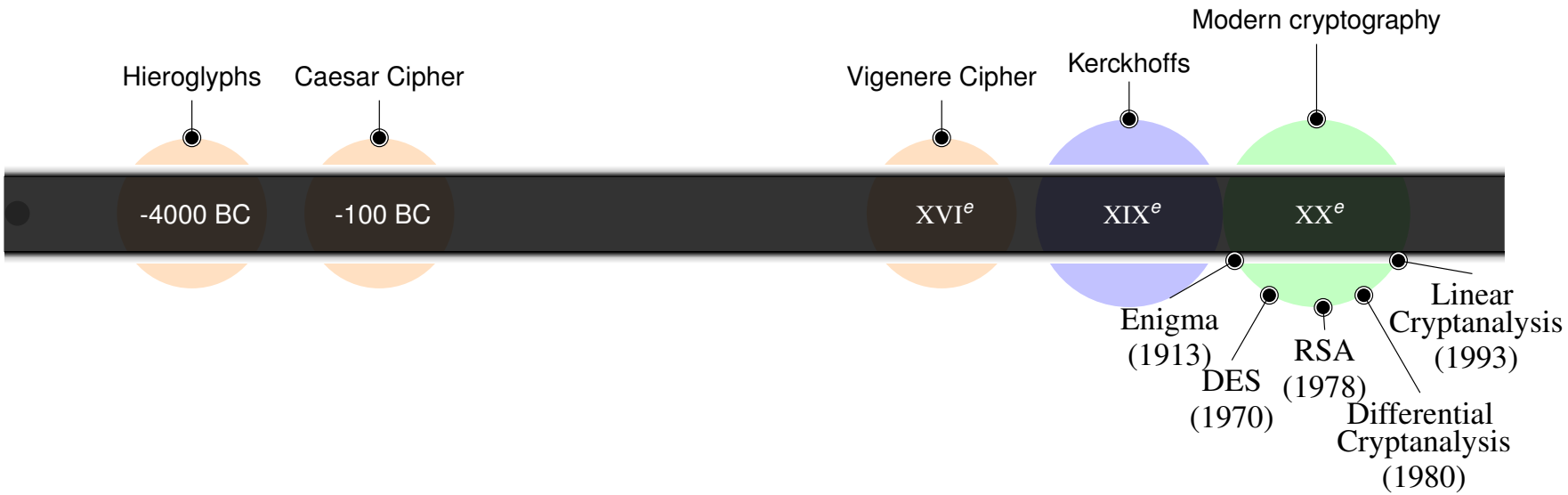
Question

How hieroglyphs had been decrypted in XIX^e century?

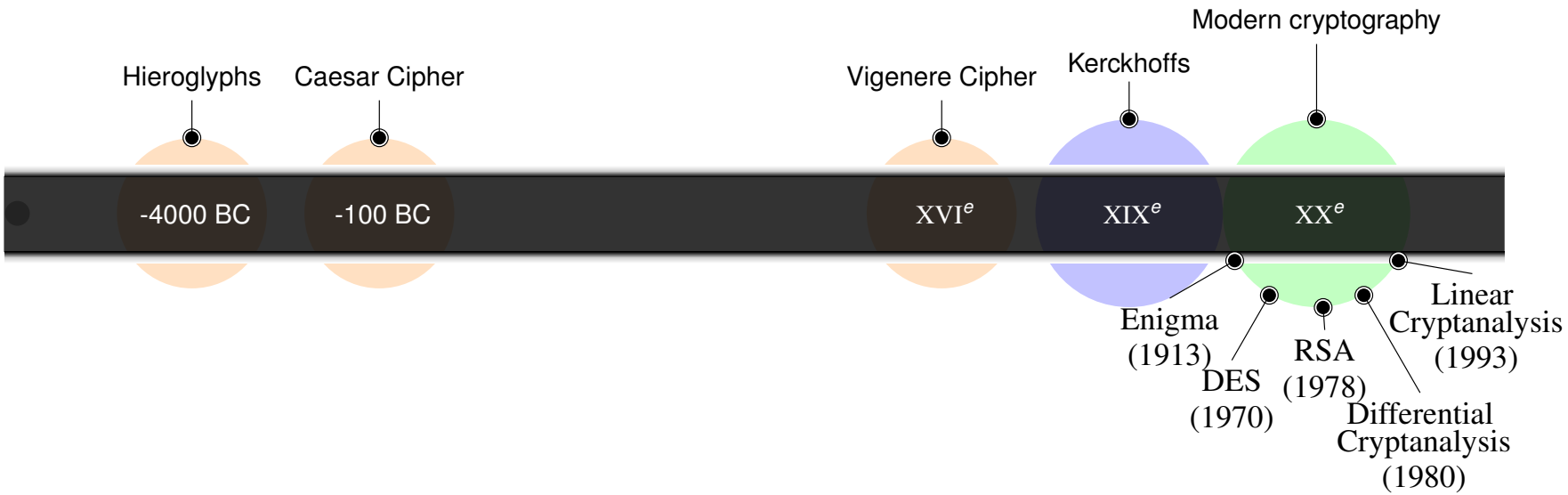
Rosetta Stone

Discovered in 1799, decree edicted in 196 before Jesus-Christ and is written in both Ancient Egyptian and Ancient Greek.

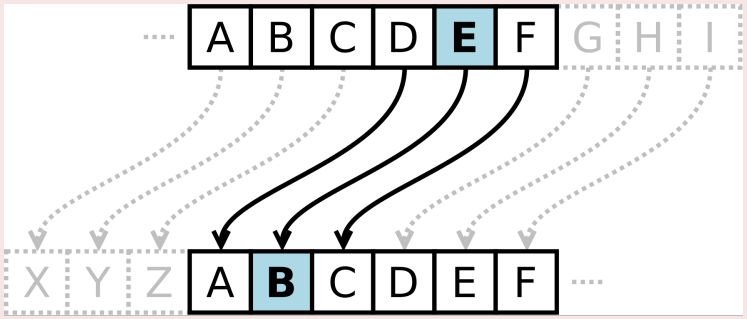
Brief History of Cryptography



Brief History of Cryptography

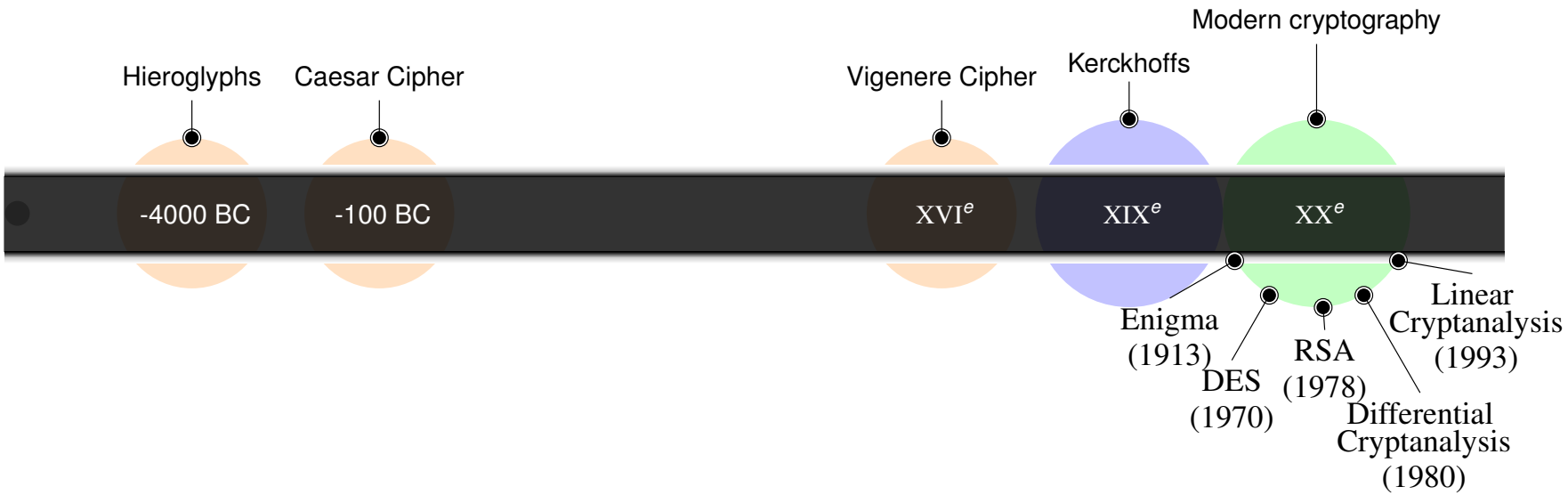


Caesar Cipher

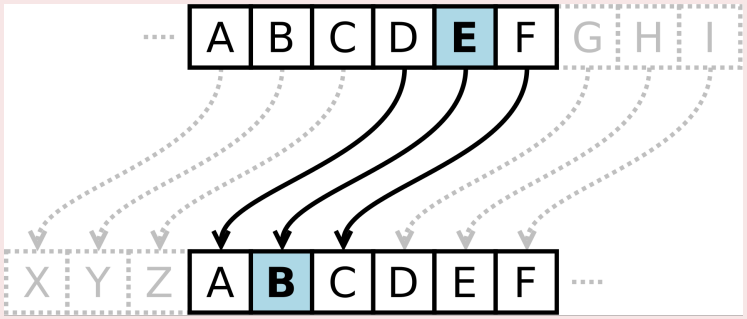


Also known as shift cipher, symbols are just shifted.
Is it secure? Why?

Brief History of Cryptography

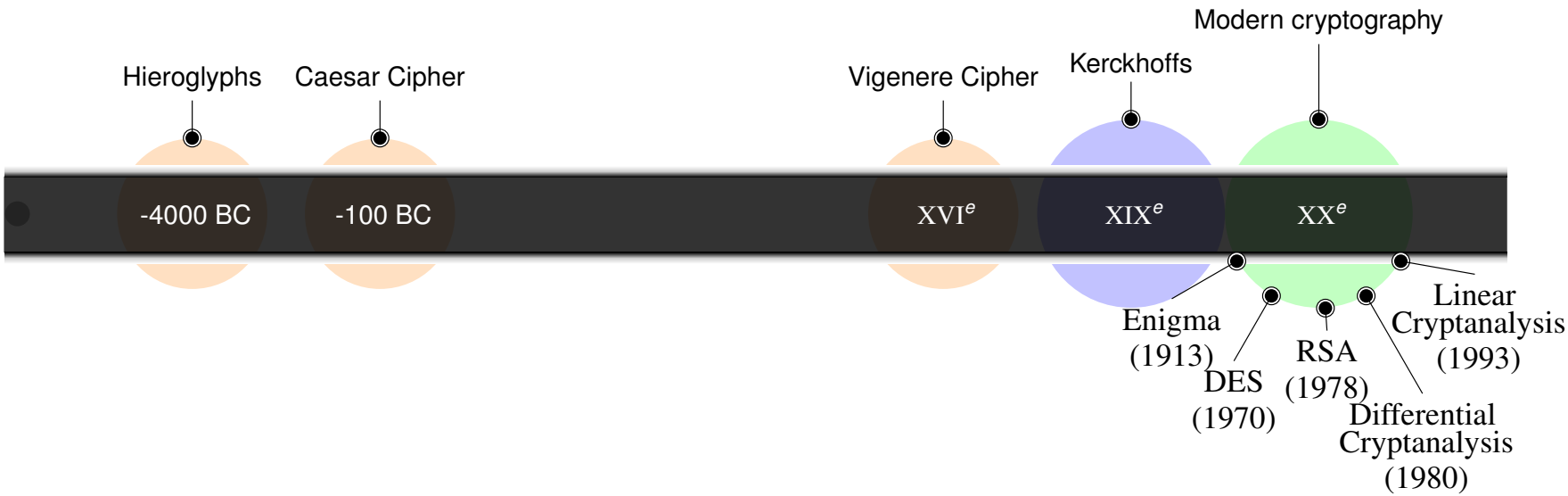


Caesar Cipher



Also known as shift cipher, symbols are just shifted. Knowing the language, cipher weak to frequency analysis.

Brief History of Cryptography

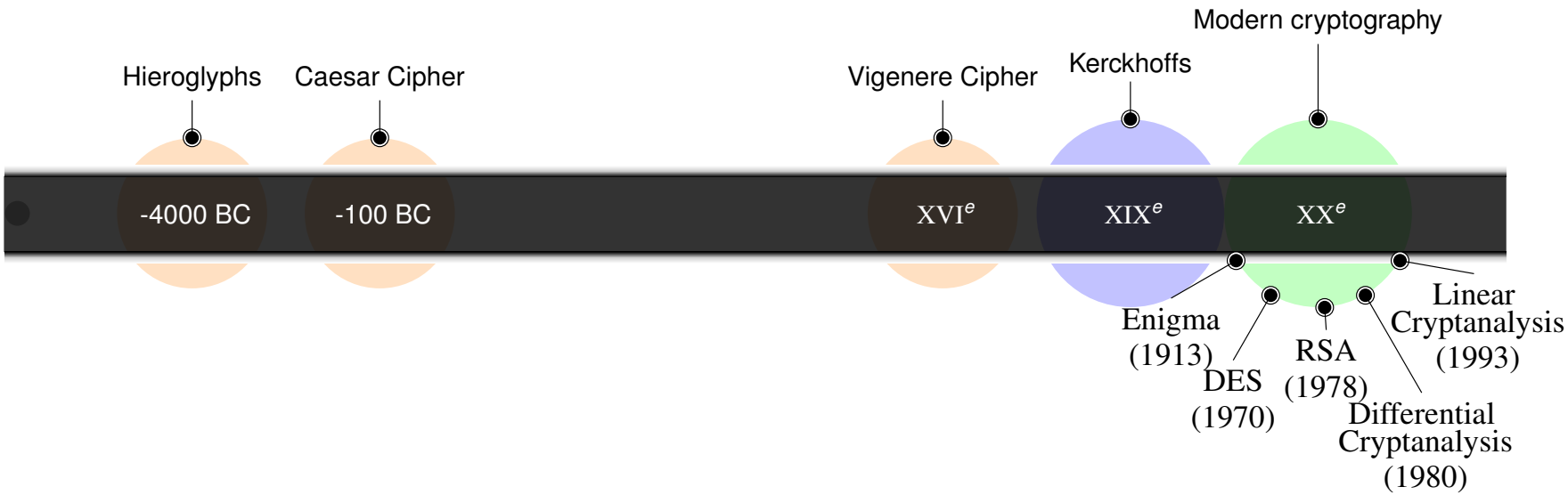


(Blaise de) Vigenère Cipher

	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

Vigenère cipher is combinaison of caesar cipher plus a variable shift provided by a secret phrase.
Defeat simple frequency analysis since a letter may be encrypted by different symbols for one ciphertext.

Brief History of Cryptography

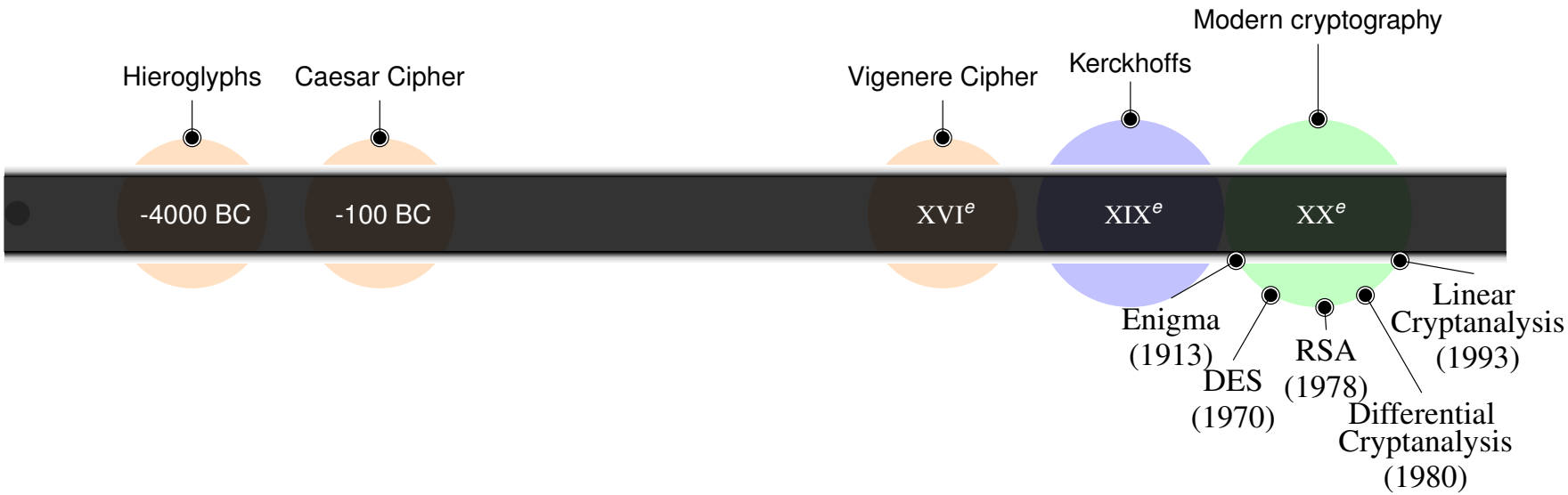


(Auguste) Kerckhoffs principles

Military cryptographier. Provided several principles that influenced modern cryptography:

- The system should be, if not theoretically unbreakable, unbreakable in practice.
- The design of a system should not require secrecy, and compromise of the system should not break security.

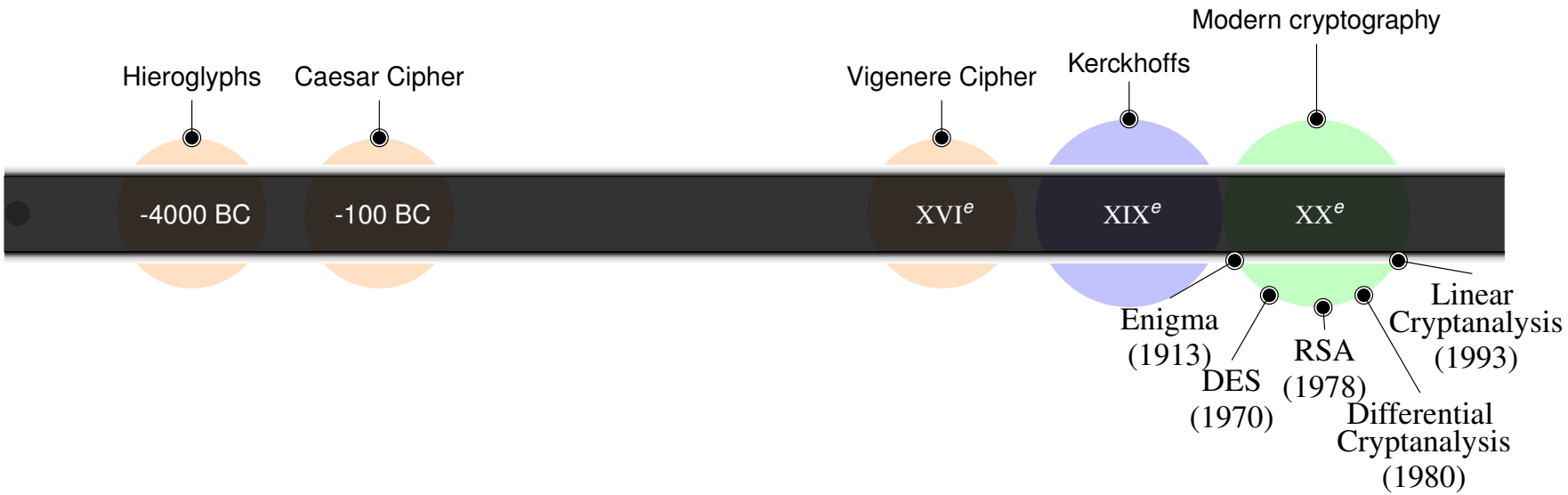
Brief History of Cryptography



Modern cryptography

- Security based on hard mathematical problems, i.e. computationally hard.
- Highly standardized, vast majority of crytosystems are public and not patented.
- Robust libraries publicly available (openSSL, libreSSL, mbedTLS, ...). Do not code your own.

Brief History of Cryptography

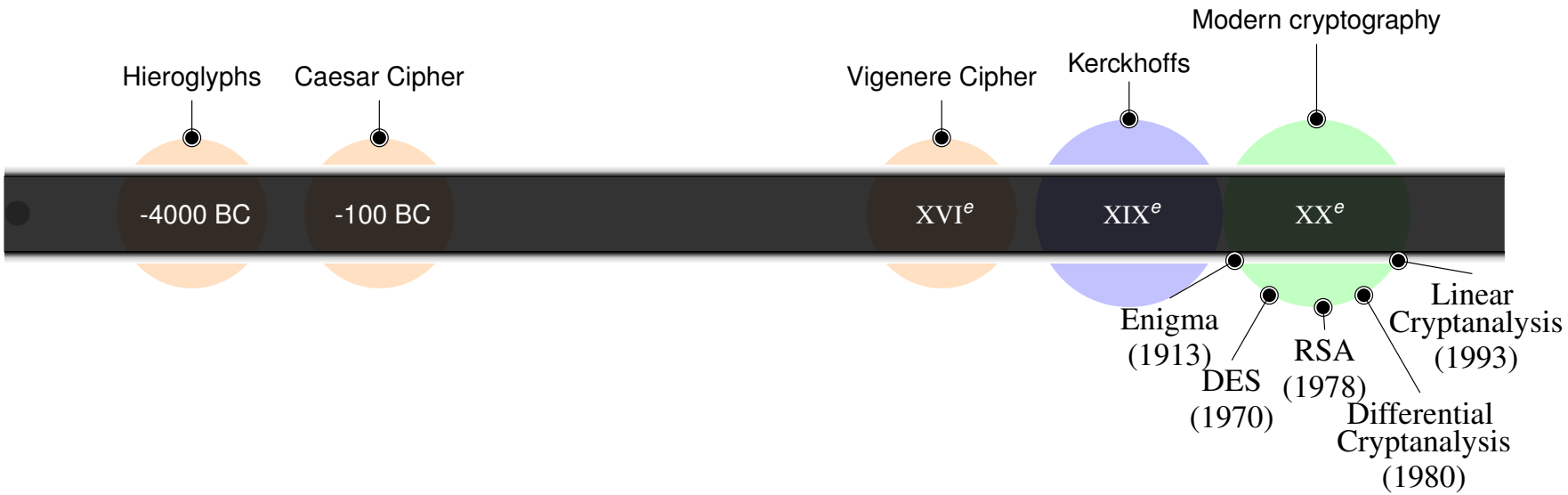


After Modern cryptography ? [1]

Several security threats are still open areas of research:

- Physical attacks:
  - Fault injection (power glitches, laser beam, spectre, meltdown, rowhammer, ...)
  - side channels (cache timing attacks, power trace analysis, ...)

Brief History of Cryptography



After Modern cryptography ? [2]

Several security threats are still open areas of research:

- Quantum computer:
  - Mostly break all “standard” asymmetric cryptography.
  - Design of “post-quantum” cryptography, i.e. can run on a usual computer, but is not break by a quantum machine.

Standardization process

Before standardization

- Algorithms are subject to a competition.
- During the competition, crypto community tries to break the algorithms.
- If community fails, then the algorithm is considered secure.
- As an example, there is almost 40 years that community tries to break RSA, and 20 years for AES.

Actors of standardization

- For cryptographic algorithm standardization:
  National Institute of Standards and Technology (NIST).
  Current competition: Post-Quantum cryptography.
- For internet protocols (TCP/IP in particular) standardization:
  Internet Engineering Task Force (IETF).
- For specific domains standardization:
  ISO.
  Example: ISO/IEC 29192 for IoT.

Standardization process

Before standardization

- Algorithms are subject to a competition.
- During the competition, crypto community tries to break the algorithms.
- If community fails, then the algorithm is considered secure.
- As an example, there is almost 40 years that community tries to break RSA, and 20 years for AES.

Actors of standardization

- For cryptographic algorithm standardization:
  National Institute of Standards and Technology (NIST).
  Current competition: Post-Quantum cryptography.
- For internet protocols (TCP/IP in particular) standardization:
  Internet Engineering Task Force (IETF).
- For specific domains standardization:
  ISO.
  Example: ISO/IEC 29192 for IoT.

Construction of cryptographic algorithms: security properties

Security properties

Usual security properties

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

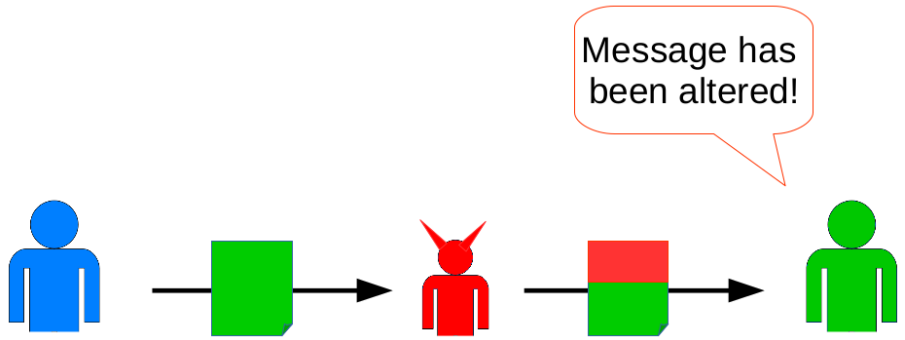
Confidentiality

If attacker intercept the ciphertext, them can't infer information about the message.

Security properties

Usual security properties

- Confidentiality
- Integrity
- Authentication
- Non-repudiation



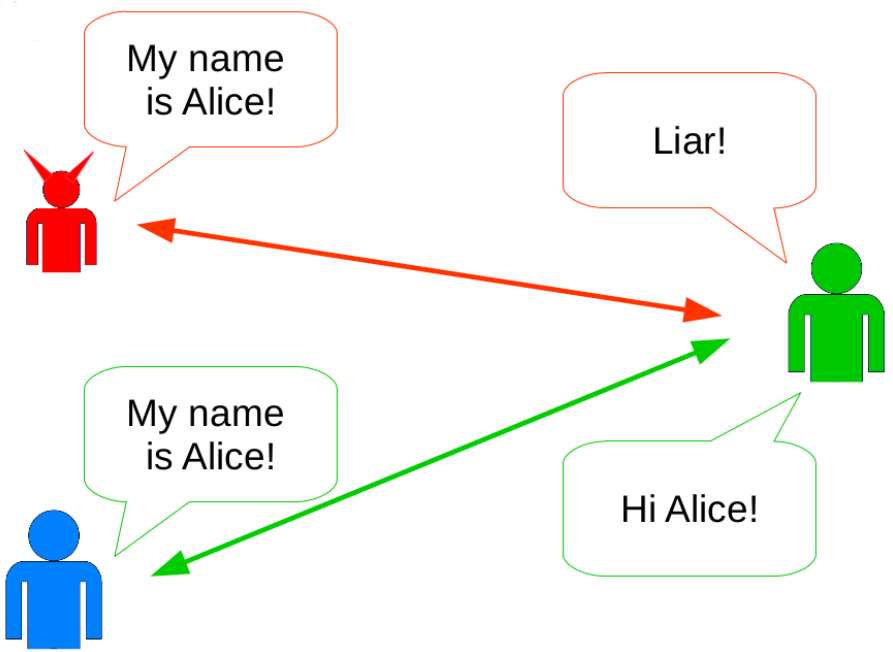
Integrity

If attacker modify the ciphertext, it can be detected by recipient.

Security properties

Usual security properties

- Confidentiality
- Integrity
- Authentication
- Non-repudiation



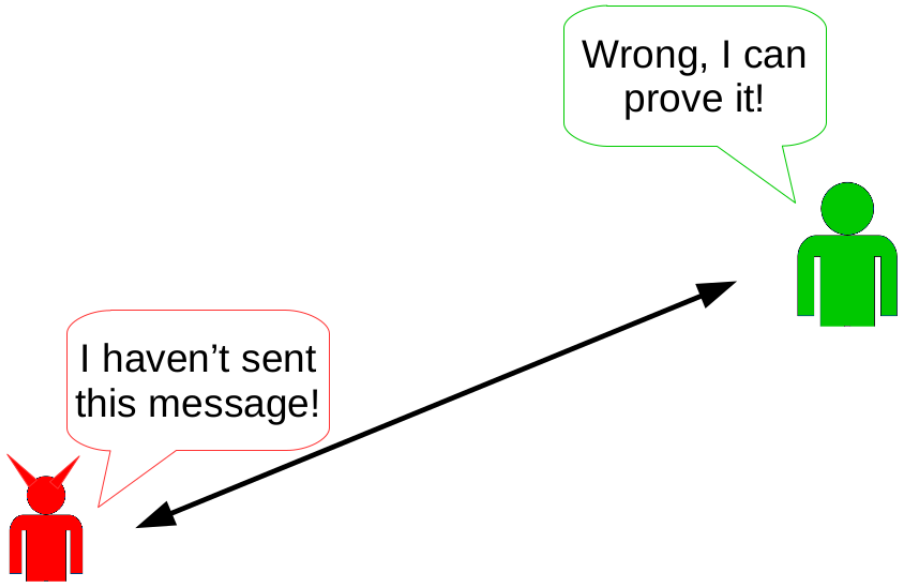
Authentication

If attacker try to impersonate someone, it can be detected by recipient.

Security properties

Usual security properties

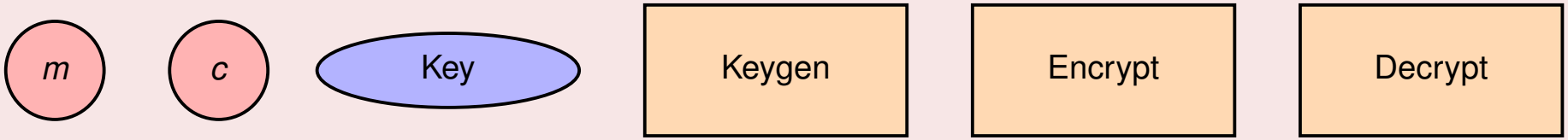
- Confidentiality
- Integrity
- Authentication
- Non-repudiation



Non-repudiation

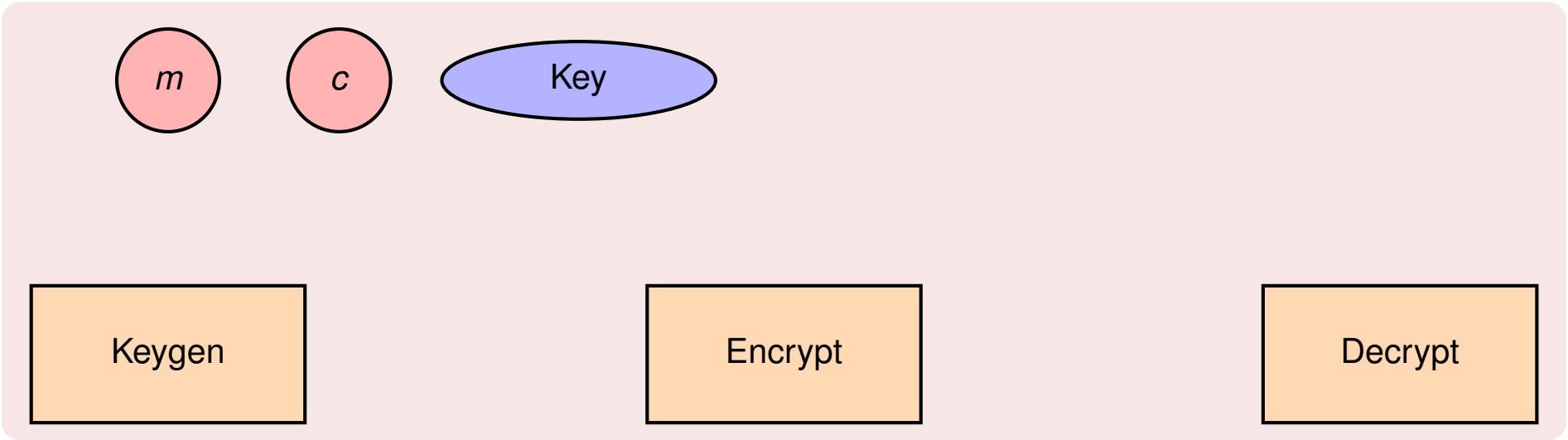
If someone tries to hide its responsability, it can be detected by recipient.

Fundamental terms



- Plaintext : unencrypted message $m \in \mathcal{M}$
- Ciphertext : encrypted message $c \in \mathcal{C}$
- Symmetric key : secret required to encrypt/decrypt $sk \in \mathcal{K}$
- Keygen : generation of the secret $c \leftarrow Keygen()$
- Encryption : generation of the ciphertext from the plaintext $c \leftarrow Enc(sk, m)$
- Decryption : extraction of the plaintext from the ciphertext $m \leftarrow Dec(sk, c)$
- Secured channel : Channel for key exchange
- Unsecured channel : Channel to send/store data

Standard constructions

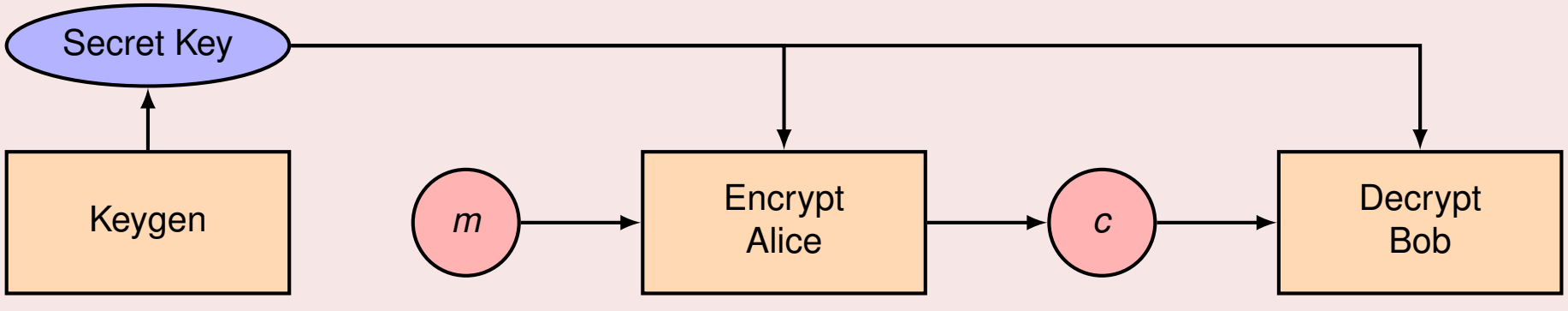


Question

- Alice wants to send a message to its boyfriend Bob.
- She also wants that Bob can verify if the message is from Alice.
- We consider that the message is not intercepted by attacker.

Complete the figure: Place *m*, *c*, *Key* (public, private, ...), Alice and Bob.

Standard constructions

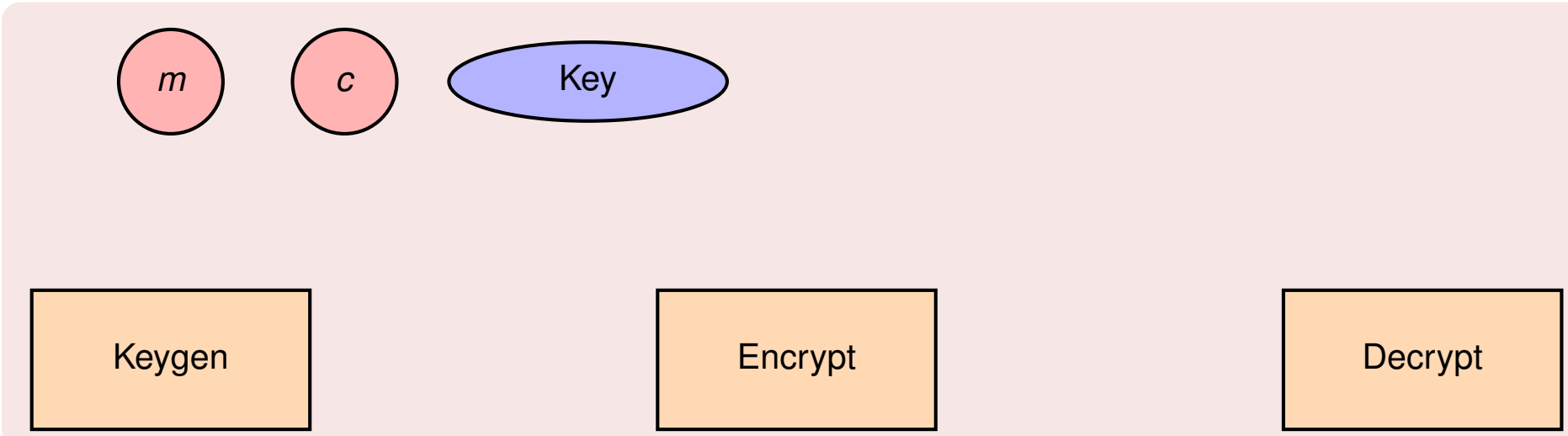


Answer

- Alice wants to send a message to its boyfriend Bob.
- She also wants that Bob can verify if the message is from Alice.
- We consider that the message is not intercepted by attacker.

If Alice and Bob use a unique secret key, then they can verify the sender.
This construction is known as Symmetric Encryption.

Standard constructions

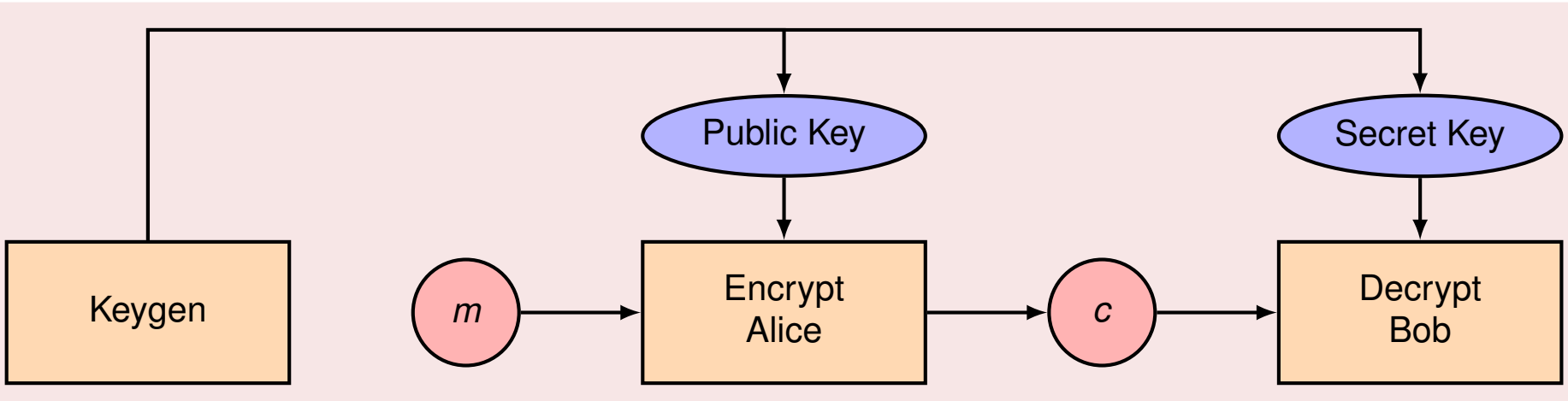


Question

- Alice wants to send a message to its boyfriend Bob.
- ~~She also wants that Bob can verify if the message is from Alice~~.
- We consider that the message is not intercepted by attacker.

Complete the figure: Place *m*, *c*, *Key* (public, private, ...), Alice and Bob.

Standard constructions

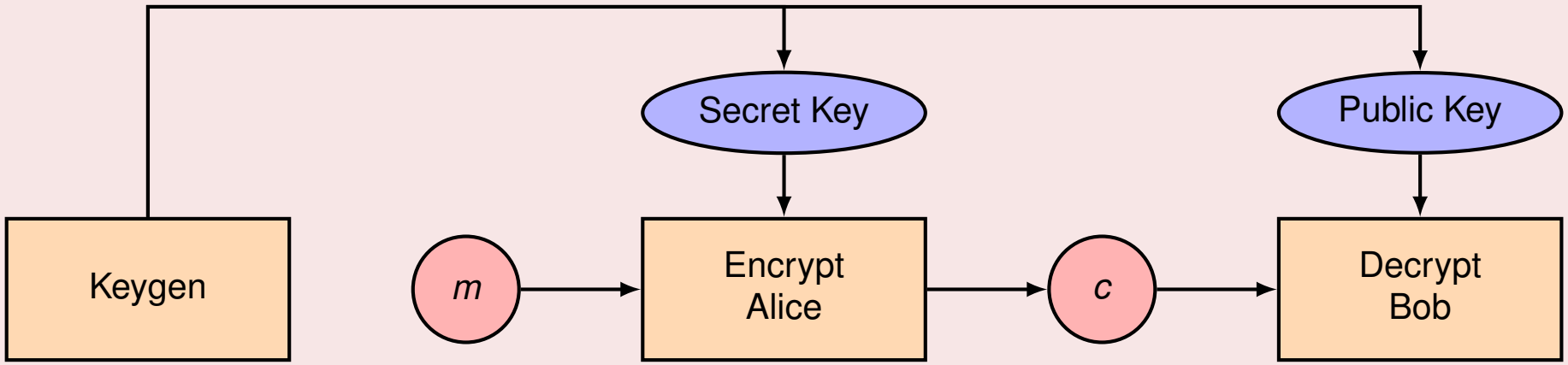


Answer

- Alice wants to send a message to its boyfriend Bob.
- ~~She also wants that Bob can verify if the message is from Alice~~.
- We consider that the message is not intercepted by attacker.

Alice dont need some kind of authentication, so encryption key can be public. However decryption must remain secret. This construction is known as Asymmetric Encryption.

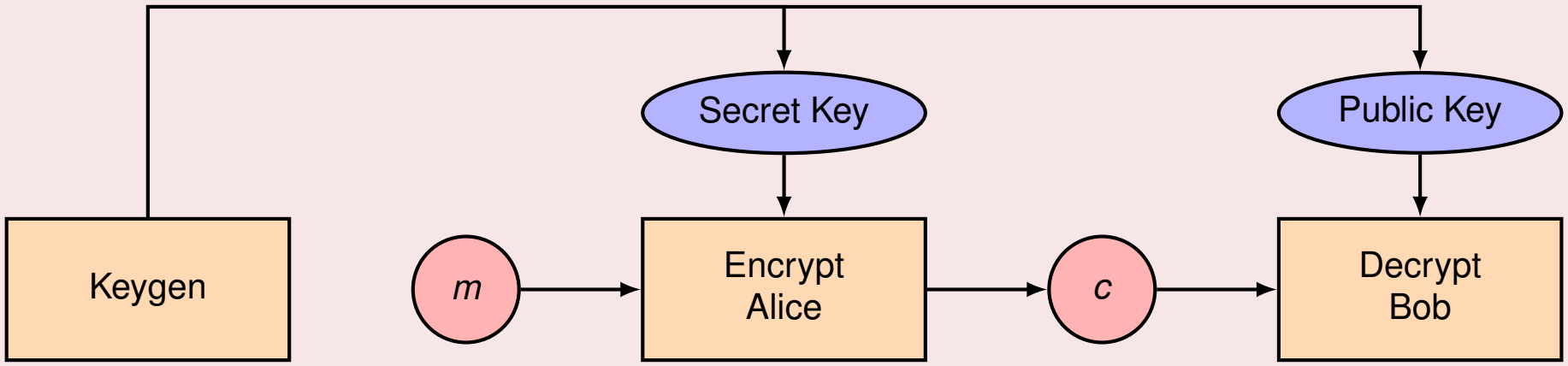
Standard constructions



Question

If Encryption key is secret and Decryption key is public, what kind of construction is it?

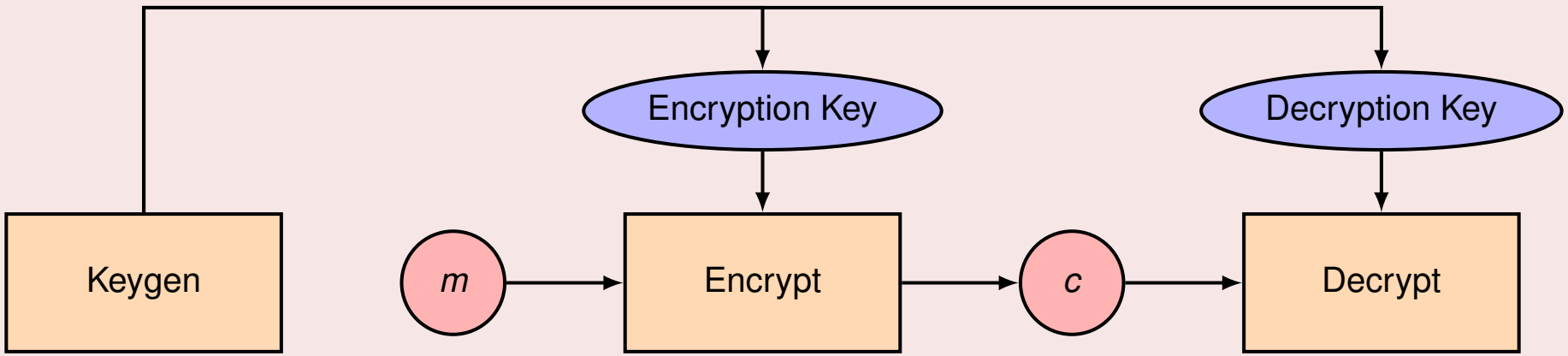
Standard constructions



Answer

In most cases, it's a building block for authentication protocols. Bob send a challenge to Alice. Alice encrypt the challenge with its secret key, and Bob verify the encryption using the Alice public key.

Functions and Algorithms



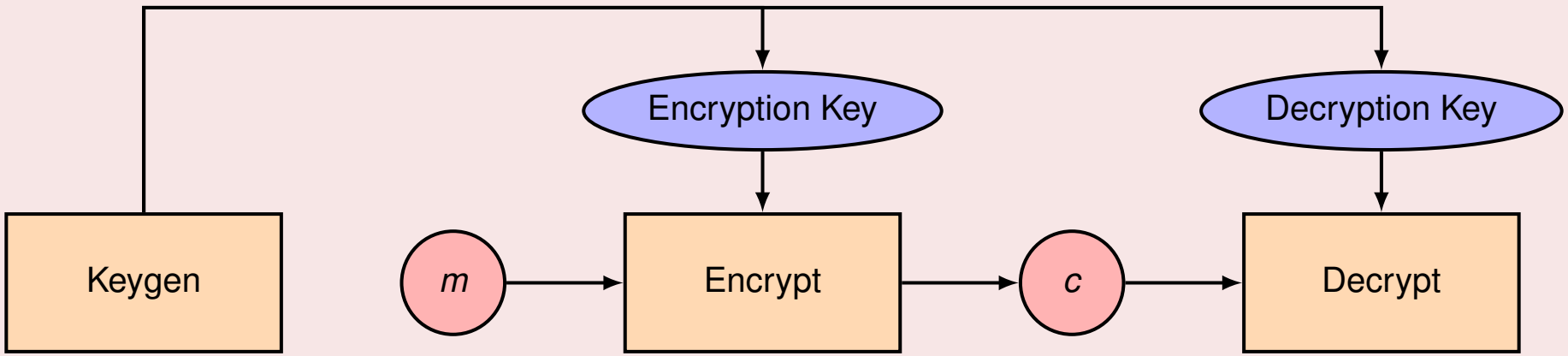
Functional notation

For function f, variable x in the field of definition of f, y is the unique output of f at point x. We note $f(x) = y$.

Deterministic Algorithms

Similarily to functions, a deterministic algorithm A have a unique output y for a given input x. We use the functional notation $A(x) = y$.
Encrypt and Decrypt are deterministic algorithms
(it is not always a desirable property, for example for replay).
Consistancy: $\forall m \in \mathcal{M}, S_k \in \mathcal{K}, Dec(Enc(m, S_k), S_k) = m$

Functions and Algorithms



Functional notation

For function f, variable x in the field of definition of f, y is the unique output of f at point x. We note $f(x) = y$.

Randomized Algorithms

Randomized Algorithm A does not have a unique output for a given input x. All possible outputs is called a *Set* (S), and a probability is associated with each element of S (called distribution χ). A random source is mandatory for such algorithms.

Keygen is a Randomized Algorithm without a specific input. In practice, Keygen is implemented as a deterministic algorithm with at leat one random

Sets and distributions

Definitions

A distribution χ over a set S is a function that associate a probability for each element of S.

Draws

We note $x \xleftarrow{\chi} S$ or $x \leftarrow (S, \chi)$ the draw of an element of S following distribution χ

Notation can be simplified to $x \leftarrow S$ when:

- χ is uniform distribution;
- there is no ambiguity that S is associated with χ.

Usual distributions

- Uniform distribution U: Same probability for each element of the set;
- Normal distribution: a high probabilty of a specific output, then probability decreases when deviate from this output(also called gaussian distribution).

Design of a symmetric encryption algorithm

INSA TOULOUSE

Notation

- Encryption of plaintext m : $c \leftarrow Enc(sk, m)$
- Decryption of ciphertext c : $m \leftarrow Dec(sk, c)$
- Consistancy : $\forall m, sk : Dec(sk, Enc(sk, m)) = \{m\}$
- Security : ciphertexts does not reveal information about plaintext or key

Which encryption provides consistancy?

$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1, 2, 3, \ldots, 255\}$

1. $Enc(k, m) = k + m$, $Dec(k, c) = c - k$
2. $Enc(k, m) = m$, $Dec(k, c) = c$
3. $Enc(k, m) = m\,[k]$, $Dec(k, c) = c \times k$

Design of a symmetric encryption algorithm

INSA TOULOUSE

Notation

- Encryption of plaintext m : $c \leftarrow Enc(sk, m)$
- Decryption of ciphertext c : $m \leftarrow Dec(sk, c)$
- Consistancy : $\forall m, sk : Dec(sk, Enc(sk, m)) = \{m\}$
- Security : ciphertexts does not reveal information about plaintext or key

Which encryption provides consistancy?

$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1, 2, 3, \ldots, 255\}$

1. $Enc(k, m) = k + m$, $Dec(k, c) = c - k$
2. $Enc(k, m) = m$, $Dec(k, c) = c$
3. $Enc(k, m) = m\,[k]$, $Dec(k, c) = c \times k$

Construction an elementary encryption algorithm

Properties of XOR

Notation

$\oplus$ = XOR = “eXclusif-OR” = “Addition modulo 2”:
$0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$

Quiz [2]: Value of $x \oplus y \oplus x$?

1. 0
2. x
3. y
4. It depends on x

How to apply it in cryptography?

Properties of XOR

Notation

$\oplus$ = XOR = “eXclusif-OR” = “Addition modulo 2”:
$0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$

Quiz [2]: Value of $x \oplus y \oplus x$?

1. 0
2. x
3. y
4. It depends on x

How to apply it in cryptography?

Simple encryption achieving perfect secrecy

One Time Pad (Vernam, 1917)

message $\oplus$ key = cipher cipher $\oplus$ key = message

```
message :  0 1 0 1 1 1 1 0 0 0 0 1 0 0 1
clé     :  1 1 0 0 0 1 0 1 0 0 0 1 1 1 0
========================================
chiffré :  1 0 0 1 1 0 1 1 0 0 0 1 1 1 1
```

Security - 1

Output distribution is uniform

$$\begin{aligned} P(c_i = 1) &= P(k_i = 1 \cap m_i = 0) + P(k_i = 0 \cap m_i = 1) \\ &= P(k_i = 1) * P(m_i = 0) + P(k_i = 0) * P(m_i = 1) \\ P(c_i = 1) &= 1/2 \end{aligned}$$

Simple encryption achieving perfect secrecy

One Time Pad (Vernam, 1917)

message $\oplus$ key = cipher cipher $\oplus$ key = message

```
message :  0 1 0 1 1 1 1 0 0 0 0 1 0 0 1
clé     :  1 1 0 0 0 1 0 1 0 0 0 1 1 1 0
========================================
chiffré :  1 0 0 1 1 0 1 1 0 0 0 1 1 1 1
```

Security - 2

For a given ciphertext, any plaintext is possible.

Simple encryption achieving perfect secrecy

One Time Pad (Vernam, 1917)

message $\oplus$ key = cipher cipher $\oplus$ key = message

```
message :   0 1
clé     :   1 1
=======================================
chiffré :   1 0
```

Security - 2

For a given ciphertext, any plaintext is possible.

Simple encryption achieving perfect secrecy

One Time Pad (Vernam, 1917)

message $\oplus$ key = cipher cipher $\oplus$ key = message

```
message :   X X
clé     :   X X
=======================================
chiffré :   1 0
```

Security - 2

For a given ciphertext, any plaintext is possible.

Simple encryption achieving perfect secrecy

One Time Pad (Vernam, 1917)

message $\oplus$ key = cipher cipher $\oplus$ key = message

```
message :   X X       0 0 | 0 1 | 1 0 | 1 1
clé     :   X X       1 0 | 1 1 | 0 0 | 0 1
=======================================
chiffré :   1 0       1 0 | 1 0 | 1 0 | 1 0
```

Security - 2

For a given ciphertext, any plaintext is possible.

Simple encryption achieving perfect secrecy

Perfect secrecy definition

Perfect Secrecy (or information-theoretic secure) means that the ciphertext conveys no information about the content of the plaintext.

Question: How to achieve perfect secrecy?

For Y ciphertext observed by attacker and X associated plaintext

1. $\forall m, c : P[X = m | Y = c] = 1/|M|$
2. $\forall m, c : P[X = m | Y = c] = P[X = m]$
3. $\forall m, c : P[X = m] = P[Y = c]$
4. $\forall m, c : P[X = m | Y = c] = 1/|K|$

Simple encryption achieving perfect secrecy

INSA TOULOUSE

Perfect secrecy definition

Perfect Secrecy (or information-theoretic secure) means that the ciphertext conveys no information about the content of the plaintext.

Question: How to achieve perfect secrecy?

For Y ciphertext observed by attacker and X associated plaintext

1. $\forall m, c : P[X = m | Y = c] = 1/|M|$
2. $\forall m, c : P[X = m | Y = c] = P[X = m]$
3. $\forall m, c : P[X = m] = P[Y = c]$
4. $\forall m, c : P[X = m | Y = c] = 1/|K|$

Simple encryption achieving perfect secrecy

INSA TOULOUSE

Perfect secrecy definition

Perfect Secrecy (or information-theoretic secure) means that the ciphertext conveys no information about the content of the plaintext.

Does OTP achieve perfect secrecy?

- $\rightarrow$ $P[A|B] = P[A \cap B]/P[B]$.
- $\rightarrow$ A, B independants $\Leftrightarrow$ $P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$.
- $\rightarrow$ $P[B] = \sum P[A_i \cap B]$ for A_i a partition of Ω.

Simple encryption achieving perfect secrecy

INSA TOULOUSE

Perfect secrecy definition

Perfect Secrecy (or information-theoretic secure) means that the ciphertext conveys no information about the content of the plaintext.

Does OTP achieve perfect secrecy?

- $\rightarrow$ $P[A|B] = P[A \cap B]/P[B]$.
- $\rightarrow$ A, B independants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$.
- $\rightarrow$ $P[B] = \sum P[A_i \cap B]$ for A_i a partition of Ω.
1. $P[X = m | Y = c] = P[X = m \cap Y = c]/P[Y = c]$

Simple encryption achieving perfect secrecy

Perfect secrecy definition

Perfect Secrecy (or information-theoretic secure) means that the ciphertext conveys no information about the content of the plaintext.

Does OTP achieve perfect secrecy?

- $\rightarrow$ $P[A|B] = P[A \cap B]/P[B]$.
- $\rightarrow$ A, B independants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$.
- $\rightarrow$ $P[B] = \sum P[A_i \cap B]$ for A_i a partition of Ω.

1. $P[X = m | Y = c] = P[X = m \cap Y = c]/P[Y = c]$
2. $P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$

Simple encryption achieving perfect secrecy

Perfect secrecy definition

Perfect Secrecy (or information-theoretic secure) means that the ciphertext conveys no information about the content of the plaintext.

Does OTP achieve perfect secrecy?

- $\rightarrow$ $P[A|B] = P[A \cap B]/P[B]$.
- $\rightarrow$ A, B independants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$.
- $\rightarrow$ $P[B] = \sum P[A_i \cap B]$ for A_i a partition of Ω.

1. $P[X = m | Y = c] = P[X = m \cap Y = c]/P[Y = c]$
2. $P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$
3. $P[Y = c] = \sum_{i \in M} P[X = i \cap K = c \oplus i] = \sum_{i \in M} P[X = i]/|K| = 1/|K|$

Simple encryption achieving perfect secrecy

Perfect secrecy definition

Perfect Secrecy (or information-theoretic secure) means that the ciphertext conveys no information about the content of the plaintext.

Does OTP achieve perfect secrecy?

- $\rightarrow$ $P[A|B] = P[A \cap B]/P[B]$.
- $\rightarrow$ A, B independants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$.
- $\rightarrow$ $P[B] = \sum P[A_i \cap B]$ for A_i a partition of Ω.

1. $P[X = m | Y = c] = P[X = m \cap Y = c]/P[Y = c]$
2. $P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$
3. $P[Y = c] = \sum_{i \in M} P[X = i \cap K = c \oplus i] = \sum_{i \in M} P[X = i]/|K| = 1/|K|$
4. $P[X = m \cap Y = c] = P[X = m \cap K = c \oplus m] = P[X = m] * 1/|K|$

Simple encryption achieving perfect secrecy

Perfect secrecy definition

Perfect Secrecy (or information-theoretic secure) means that the ciphertext conveys no information about the content of the plaintext.

Does OTP achieve perfect secrecy?

- $\rightarrow$ $P[A|B] = P[A \cap B]/P[B]$.
- $\rightarrow$ A, B independants $\Leftrightarrow P[A \cap B] = P[A] * P[B] \Leftrightarrow P[A|B] = P[A]$.
- $\rightarrow$ $P[B] = \sum P[A_i \cap B]$ for A_i a partition of Ω.

1. $P[X = m | Y = c] = P[X = m \cap Y = c]/P[Y = c]$
2. $P[Y = c] = \sum_{i \in M} P[X = i \cap Y = c]$
3. $P[Y = c] = \sum_{i \in M} P[X = i \cap K = c \oplus i] = \sum_{i \in M} P[X = i]/|K| = 1/|K|$
4. $P[X = m \cap Y = c] = P[X = m \cap K = c \oplus m] = P[X = m] * 1/|K|$
5. $P[X = m | Y = c] = P[X = m \cap Y = c]/P[Y = c]$

Is OTP a perfect solution?

Perfect secrecy ... but not practical

Maleability

If an attacker intercepts ciphertext c of a message m and computes $c' = c \oplus x$ then c' is a valid ciphertext of message $m' = m \oplus x$

Key management

Key cant be used twice!!

$c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$

Bad news

Shanon theorem

If encryption algorithm achieves perfect secrecy, then $|K| \geq |M|$

Proof

Proof by contradiction: we consider $|K| < |M|$ and an attacker studies $Y = c$
When trying brute force by testing all possible keys,
$M_0 = \cup_{k \in K} Dec(k, c) \implies |M_0| < |M|$
$\Rightarrow$ for $m \notin M_0$, $P[X = m \mid Y = c] = 0$ event if $P[X = m] = 1/|M|$

OTP: Maleability

Context

Alice and Bob agree on a key, they want to send a “Y” or “N” message (i.e. yes or no) using OTP. Eve intercept ciphertext c and tries to switch message from “Y” to “N” and vice versa. Feasible?

OTP: Maleability

Context

Alice and Bob agree on a key, they want to send a “Y” or “N” message (i.e. yes or no) using OTP. Eve intercept ciphertext *c* and tries to switch message from “Y” to “N” and vice versa. Feasible?

Solution

c’ = c $\oplus$ (“Y” $\oplus$ “N”)

OTP: Secret sharing

Sharing with two people

Alice knows a secret $x \in M$ that allow to launch a nuclear missile.
She generate $y \xleftarrow{U} M$ et provides:

- $x \oplus y$ to her mom
- y to her dad

Mom et dad can't make a nuclear war individually.

Which of these assertions are true?

1. y is uniformly distributed over M
2. $x \oplus y$ is uniformly distributed over M
3. $(y, x \oplus y)$ is uniformly distributed over $M \times M$

OTP: Secret sharing

Sharing with two people

Alice knows a secret $x \in M$ that allow to launch a nuclear missile.
She generate $y \xleftarrow{U} M$ et provides:

- $x \oplus y$ to her mom
- y to her dad

Mom et dad can't make a nuclear war individually.

Which of these assertions are true?

1. y is uniformly distributed over M
2. $x \oplus y$ is uniformly distributed over M
3. $(y, x \oplus y)$ is uniformly distributed over $M \times M$

From unpractical OTP to practical encryption

End of Lesson Quiz

INSA TOULOUSE

Question

Which of these encryption algorithms vulnerable to frequency analysis?

- Caesar cipher.
- Vigenère cipher.

End of Lesson Quiz

Question

Which of these encryption algorithms vulnerable to frequency analysis?

- Caesar cipher.
- Vigenère cipher.

Answer

Caesar code.

End of Lesson Quiz

INSA TOULOUSE

Question

What are the two main turning points in cryptography?

End of Lesson Quiz

INSA TOULOUSE

Question

What are the two main turning points in cryptography?

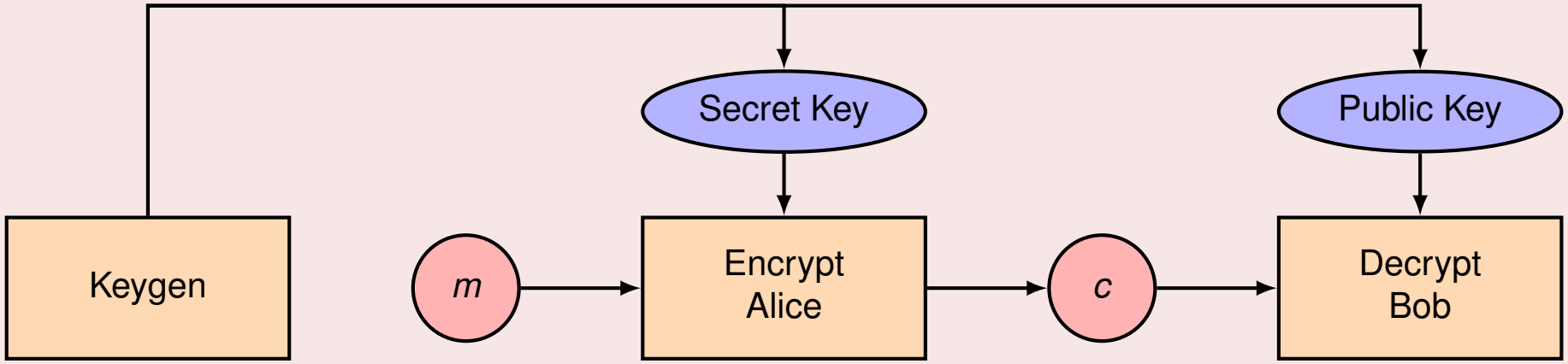
Answer

- Kerckhoffs: From AD-HOC solutions to mathematically-based solutions.
- Industrialization of calculators.

End of Lesson Quiz

Question

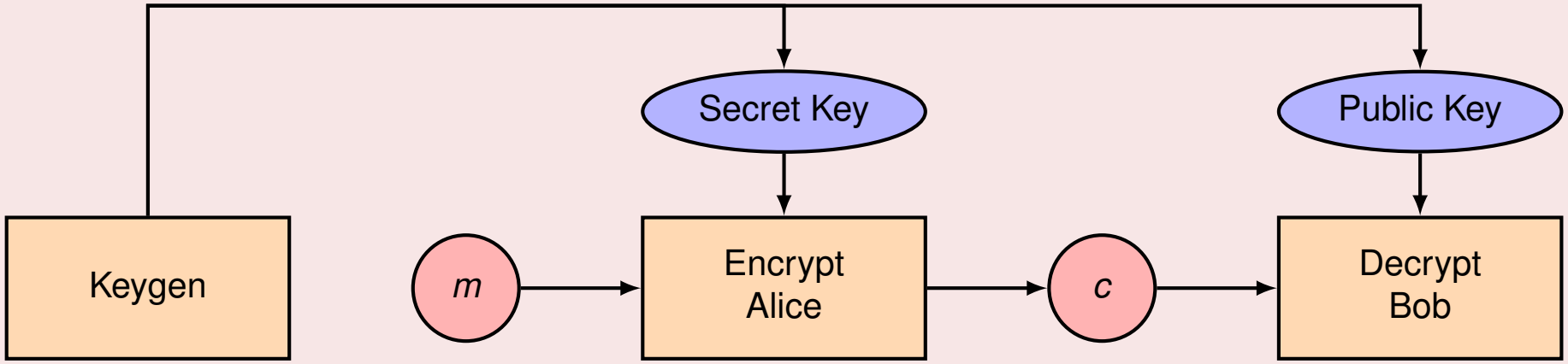
In which context this construction may be used?



End of Lesson Quiz

Question

In which context this construction may be used?



Answer

For authentication. *m* should be provided by Bob in practice, also called challenge.

References

Electronic Books:

Cornell, https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf
Bristol, http://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf
Stanford, http://crypto.stanford.edu/~dabo/cryptobook/

Online courses:

[1] Stanford, https://www.coursera.org/course/crypto
[2] Univ. of Virginia, http://www.udacity.com/view#Course/cs387/