



HAL
open science

Security and Cryptography just by images

Pascal Lafourcade

► **To cite this version:**

Pascal Lafourcade. Security and Cryptography just by images. Doctoral. Grenoble, France. 2009, pp.52. hal-04449291

HAL Id: hal-04449291

<https://uca.hal.science/hal-04449291>

Submitted on 9 Feb 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Security and Cryptography just by images

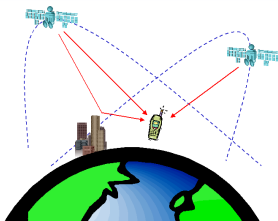
Pascal Lafourcade



2009

pascal.lafourcade@imag.fr

Applications



Secrecy or Confidentiality

Alice communicates with the White rabbit via a network.



Secrecy or Confidentiality

Alice communicates with the White rabbit via a network.



Intruder



Secrecy or Confidentiality

Alice communicates with the White rabbit via a network.



Intruder



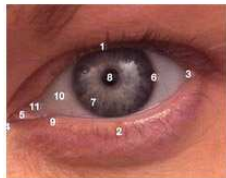
Authentication



"On the Internet, nobody knows you're a dog."

Mechanisms for Authentication

1. Something that you know
E.g. a PIN or a password
2. Something that you have
E.g. a smart-card
3. Something that you are
Biometric characteristics like voice, fingerprints, eyes, ...
4. Where you are located
E.g. in a secure building



Strong authentication combines multiple factors:
E.g., Smart-Card + PIN

Other security properties

- ▶ **Integrity**: No improper modification of information
- ▶ **Availability**: No improper impairment of functionality/service
- ▶ **Non-repudiation** (also called **accountability**) is where one can establish responsibility for actions.
- ▶ **Privacy** or **Anonymity**: secrecy of principal identities or communication relationships.
- ▶ etc ...

Symmetric key and public key encryption

- Symmetric key encryption



- Public key encryption



Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

Logical Attacks

Interactive Zero Knowledge Proofs

Secret Sharing

Conclusion

Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

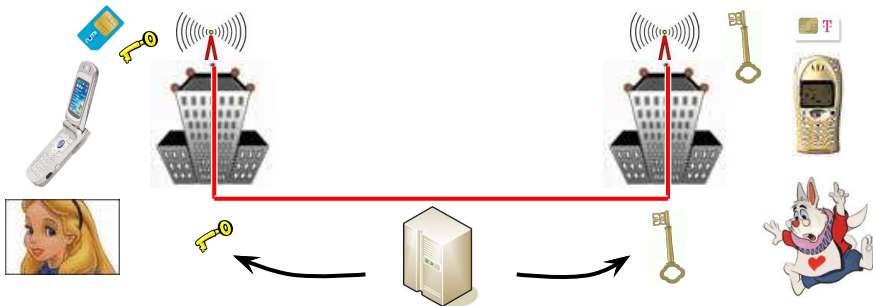
Logical Attacks

Interactive Zero Knowledge Proofs

Secret Sharing

Conclusion

Symmetric Encryption for GSM communication



SIM card contains a shared secret key used for authenticating phones and operators, then creating key session for communication.

1. Message is encrypted and sent by Alice.
2. The antenna receives the message then unencrypted.
3. Message is encrypted by the antenna with the second key.
4. Second mobile unencrypted the communication.

Hash Functions

A hash function H takes as input a bit-string of any finite length and returns a corresponding 'digest' of **fixed length**.

$$H : \{0, 1\}^* \rightarrow \{0, 1\}^n$$

$$H(\textit{Alice}) = \img alt="Barcode representing the hash of Alice" data-bbox="424 458 593 574"/> \neq H(\textit{Bob})$$

marion → 

marine →  ← *laurence*

Hash function, e.g. Software Installation



Integrity of the downloaded file.

1. Download on server 1 the software.
2. Download on server 2 the hash of the software.
3. Check the integrity of the software.

Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

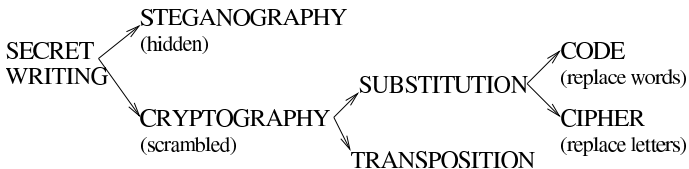
Logical Attacks

Interactive Zero Knowledge Proofs

Secret Sharing

Conclusion

Information hiding



- ▶ **Cryptology**: the study of secret writing.
- ▶ **Steganography**: the science of hiding messages in other messages.
- ▶ **Cryptography**: the science of secret writing.
Note: terms like **encrypt**, **encode**, and **encipher** are often (loosely and wrongly) used interchangeably

Slave



Historical ciphers

- ▶ Used 4000 years ago by Egyptians to encipher hieroglyphics.



- ▶ 2000 years ago Julius Caesar used a simple substitution cipher.
- ▶ Leon Alberti devised a cipher wheel, and described the principles of frequency analysis in the 1460s.

Substitution cipher examples

- ▶ L oryh brx

Substitution cipher examples

- ▶ L oryh brx = I LOVE YOU

Caesar cipher: each plaintext character is replaced by the character three to the right modulo 26.

Substitution cipher examples

- ▶ L oryh brx = I LOVE YOU
Caesar cipher: each plaintext character is replaced by the character three to the right modulo 26.
- ▶ Zngurzngvdhrf = Mathematiques
ROT13: shift each letter by 13 places.
Under Unix: `tr a-zA-Z n-za-mN-ZA-M`.
- ▶ 2-25-5 2-25-5

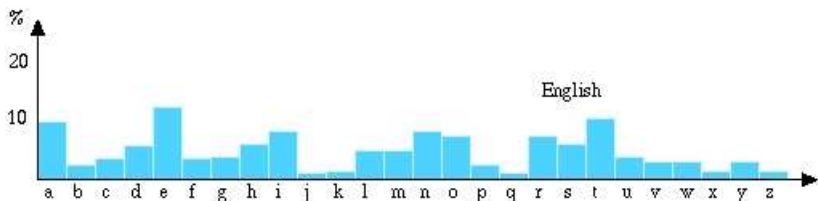
Substitution cipher examples

- ▶ L oryh brx = I LOVE YOU
Caesar cipher: each plaintext character is replaced by the character three to the right modulo 26.
- ▶ Zngurzngvdhrf = Mathematiques
ROT13: shift each letter by 13 places.
Under Unix: `tr a-zA-Z n-za-mN-ZA-M`.
- ▶ 2-25-5 2-25-5 = BYE BYE
Alphanumeric: substitute numbers for letters.

How hard are these to cryptanalyze? Caesar? General?

(In)security of substitution ciphers

- ▶ Key spaces are typically huge. 26 letters \rightsquigarrow 26! possible keys.
- ▶ Trivial to crack using frequency analysis (letters, digraphs...)
- ▶ Frequencies for English based on data-mining books/articles.



Improvement: Homophonic substitution ciphers

$$\mathcal{A} = \{a, b\}$$

$$H(a) = \{00, 10\}, \text{ and } H(b) = \{01, 11\}.$$

Example

The plaintext ab encrypts to one of 0001, 0011, 1001, 1011.

Improvement: Homophonic substitution ciphers

$$\mathcal{A} = \{a, b\}$$

$$H(a) = \{00, 10\}, \text{ and } H(b) = \{01, 11\}.$$

Example

The plaintext ab encrypts to one of 0001, 0011, 1001, 1011.

- ▶ Rational: makes frequency analysis more difficult.
- ▶ Cost: data expansion and more work for decryption.

Polyalphabetic substitution (Leon Alberti, Vignere)



Example: English ($n = 26$), with $k = 3,7,10$

$m =$ THI SCI PHE RIS CER TAI NLY NOT SEC URE

then

$E_e(m) =$ WOS VJS SOO UPC FLB WHS QSI QVD VLM XYO

Example: transposition ciphers

▶ $C = \text{Aduaenttlydhatoiekounletmtoiha hvsekeeeleeyqonouv}$

Example: transposition ciphers

- $C = \text{Aduaenttlydhatoiekounletmtoiha hvsekeeeleeyqonouv}$

A	n	d	i	n	t	h	e	e	n
d	t	h	e	l	o	v	e	y	o
u	t	a	k	e	i	s	e	q	u
a	l	t	o	t	h	e	l	o	v
e	y	o	u	m	a	k	e		

Table defines a permutation on $1, \dots, 50$.

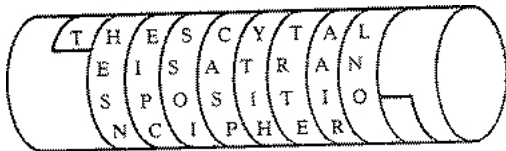
Example: transposition ciphers

- ▶ $C = \text{Aduaenttlydhatoiekounletmtoiha hvsekeeeleyqonouv}$

A	n	d	i	n	t	h	e	e	n
d	t	h	e	l	o	v	e	y	o
u	t	a	k	e	i	s	e	q	u
a	l	t	o	t	h	e	l	o	v
e	y	o	u	m	a	k	e		

Table defines a permutation on $1, \dots, 50$.

- ▶ Idea goes back to Greek **Scytale**: wrap belt spirally around baton and write plaintext lengthwise on it.



Composite ciphers

- ▶ Ciphers based on just substitutions or transpositions are not secure
- ▶ Ciphers can be combined. However . . .
 - ▶ two substitutions are really only one more complex substitution,
 - ▶ two transpositions are really only one transposition,
 - ▶ but a substitution followed by a transposition makes a new harder cipher.
- ▶ Product ciphers chain substitution-transposition combinations.
- ▶ Difficult to do by hand
↪ invention of cipher machines.



One-time pad (Vernam cipher)

N	I	N	E
N	I	N	E
I	I	N	E



One-time pad (Vernam cipher)



N	I	N	E
N	I	I	I
I	I	N	E

$$m = 010111$$

► Example: $k = 110010$

$$c = 100101$$

- Unconditional (information theoretic) security, if key isn't reused!
- Problem?

One-time pad (Vernam cipher)



N I N E
N I I I
I I N E

▶ Example:

$$\begin{array}{r} m = 010111 \\ k = 110010 \\ \hline c = 100101 \end{array}$$

- ▶ Unconditional (information theoretic) security, if key isn't reused!
- ▶ Problem? Securely exchanging and synchronizing long keys.

Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

Logical Attacks

Interactive Zero Knowledge Proofs

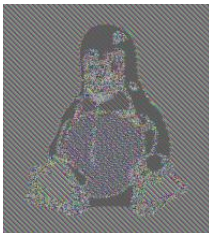
Secret Sharing

Conclusion

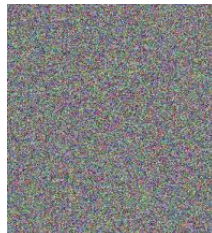
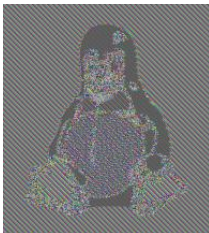
ECB vs Others



ECB vs Others



ECB vs Others



One-Wayness (OW)

Put your message in a translucent bag, but you cannot read the text.



One-Wayness (OW)

Put your message in a translucent bag, but you cannot read the text.



Without the private key, it is computationally **impossible to recover the plain-text.**

Is it secure ?



Is it secure ?



Is it secure ?



- ▶ you cannot read the text but you can distinguish which one has been encrypted.

Indistinguishability (IND)

Put your message in a black bag, you can not read anything.



Now a black bag is of course IND and it implies OW.

Is it secure?



Is it secure?



Is it secure?



- ▶ It is possible to scramble it in order to produce a new cipher. In more you know the relation between the two plain text because you know the moves you have done.

Non Malleability (NM)

Put your message in a black box.



But in a black box you cannot touch the cube (message), hence NM implies IND.

Summary of Security Notions

Non Malleability



Indistinguishability



One-Wayness



Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

Logical Attacks

Interactive Zero Knowledge Proofs

Secret Sharing

Conclusion

Attacks

Computational Model
Cryptanalysis



Attacks

Computational Model Cryptanalysis



Attacks

Computational Model
Cryptanalysis



Symbolic Model
Logical Attack

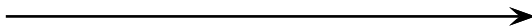
Perfect Encryption hypothesis

Needham-Schroeder Public Key Protocol (1978)

“Man in the middle attack” [Lowe'96]



Simple Example

 $\{12h10\}_{K_B}$ 

Simple Example

 $\{12h10\}_{K_B}$  $\{12h10\}_{K_B}$ 

Simple Example

 $\{12h10\}_{K_B}$  $\{12h10\}_{K_B}$ 

Day After

 $\{11h45\}_{K_B}$  $\{12h10\}_{K_B}$ 

Simple Example

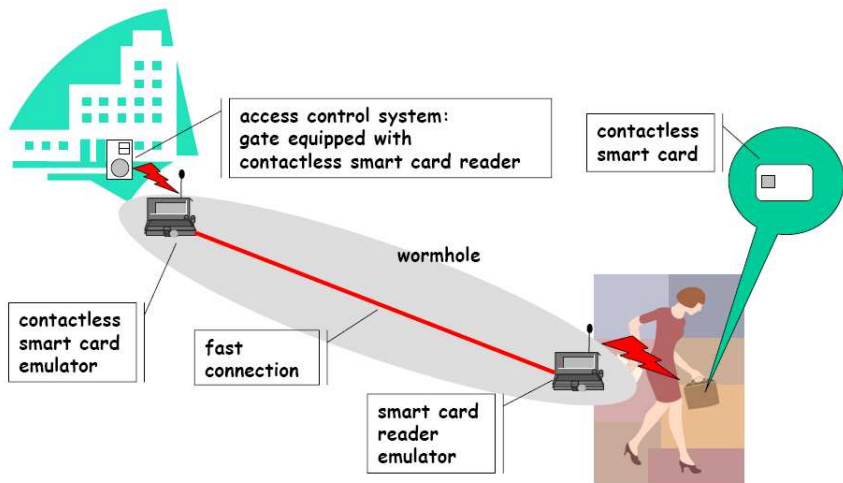
 $\{12h10\}_{K_B}$  $\{12h10\}_{K_B}$ 

Day After

 $\{11h45\}_{K_B}$  $\{12h10\}_{K_B}$ 

This kind of attack is valid for all encryptions

Authentication Problem: Wormhole Attack

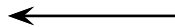


Example: Needham-Schroeder Protocol 1978

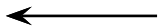
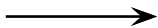
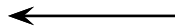

$$\{A, N_A\}_{K_B}$$


Example: Needham-Schroeder Protocol 1978

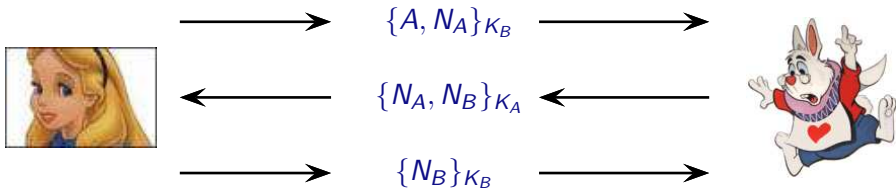

$$\{A, N_A\}_{K_B}$$

$$\{N_A, N_B\}_{K_A}$$


Example: Needham-Schroeder Protocol 1978

 $\{A, N_A\}_{K_B}$  $\{N_A, N_B\}_{K_A}$  $\{N_B\}_{K_B}$ 

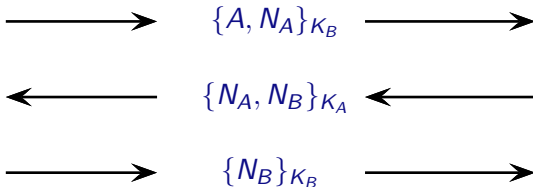
Example: Needham-Schroeder Protocol 1978



Question

- ▶ Is N_B a shared secret between A et B ?

Example: Needham-Schroeder Protocol 1978



Question

- ▶ Is N_B a shared secret between A et B ?

Answer

- ▶ In 1995, G.Lowe find an attack **17 years** after its publication!

Lowé Attack on the Needham-Schroeder

so-called “Man in the middle attack”



Agent A



Intruder I



Agent B

$$\begin{aligned}
 A &\longrightarrow B : \{A, N_a\}_{K_B} \\
 B &\longrightarrow A : \{N_a, N_b\}_{K_A} \\
 A &\longrightarrow B : \{N_b\}_{K_B}
 \end{aligned}$$

Low Attack on the Needham-Schroeder

so-called “Man in the middle attack”



Agent A

$$\{A, N_a\}_{K_I}$$


Intruder I

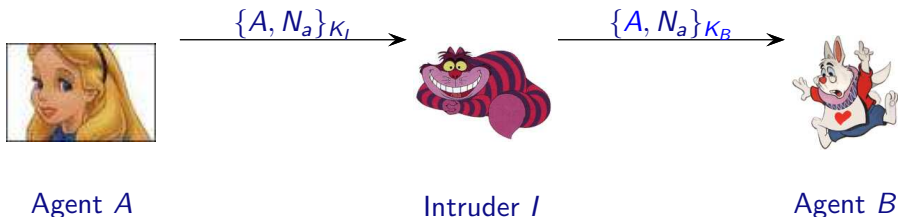


Agent B

- $A \longrightarrow B : \{A, N_a\}_{K_B}$
- $B \longrightarrow A : \{N_a, N_b\}_{K_A}$
- $A \longrightarrow B : \{N_b\}_{K_B}$

Low Attack on the Needham-Schroeder

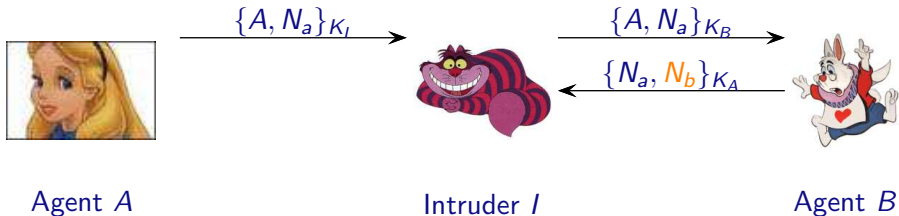
so-called “Man in the middle attack”



- $A \longrightarrow B : \{A, N_a\}_{K_B}$
 $B \longrightarrow A : \{N_a, N_b\}_{K_A}$
 $A \longrightarrow B : \{N_b\}_{K_B}$

Low Attack on the Needham-Schroeder

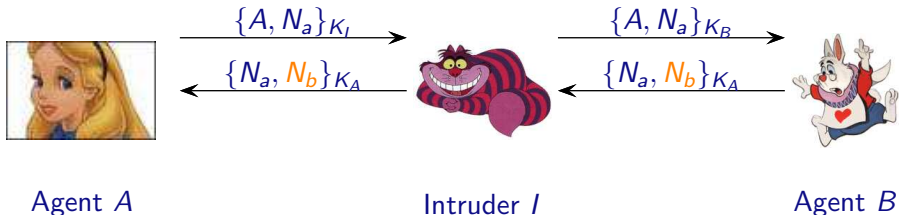
so-called "Man in the middle attack"



- $A \longrightarrow B : \{A, N_a\}_{K_B}$
 $B \longrightarrow A : \{N_a, N_b\}_{K_A}$
 $A \longrightarrow B : \{N_b\}_{K_B}$

Lowé Attack on the Needham-Schroeder

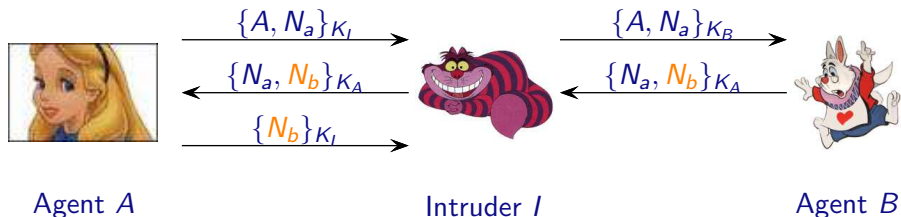
so-called “Man in the middle attack”



- $A \longrightarrow B : \{A, N_a\}_{K_B}$
 $B \longrightarrow A : \{N_a, N_b\}_{K_A}$
 $A \longrightarrow B : \{N_b\}_{K_B}$

Lowé Attack on the Needham-Schroeder

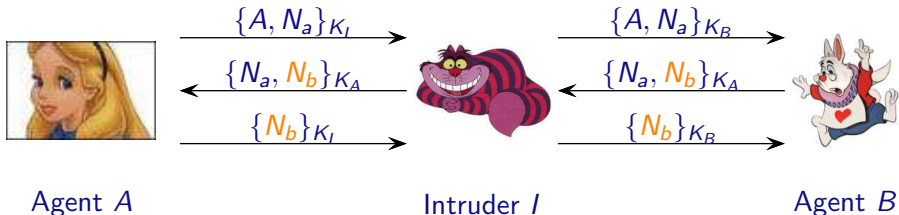
so-called "Man in the middle attack"



- $A \longrightarrow B : \{A, N_a\}_{K_B}$
- $B \longrightarrow A : \{N_a, N_b\}_{K_A}$
- $A \longrightarrow B : \{N_b\}_{K_B}$

Lowé Attack on the Needham-Schroeder

so-called “Man in the middle attack”

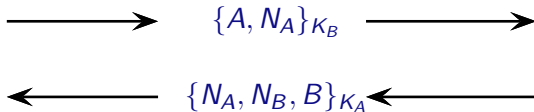


- $A \longrightarrow B : \{A, N_a\}_{K_B}$
- $B \longrightarrow A : \{N_a, N_b\}_{K_A}$
- $A \longrightarrow B : \{N_b\}_{K_B}$

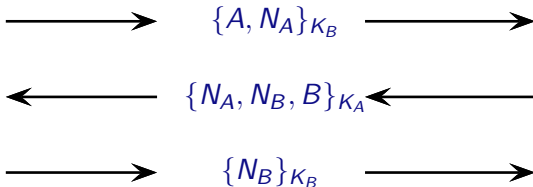
Needham-Schroeder corrected by Lowe 1995

 $\{A, N_A\}_{K_B}$ 

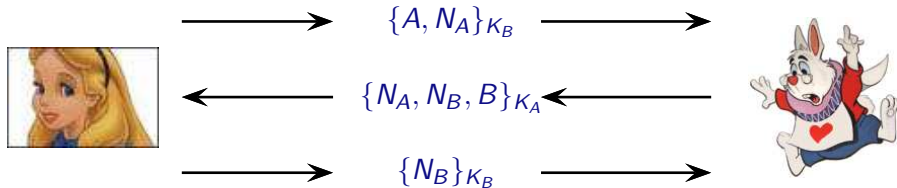
Needham-Schroeder corrected by Lowe 1995



Needham-Schroeder corrected by Lowe 1995



Needham-Schroeder corrected by Lowe 1995



Question

- ▶ This time the protocol is secure?

Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

Logical Attacks

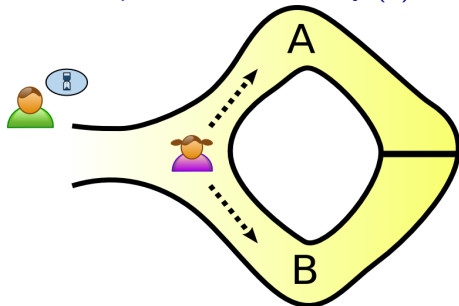
Interactive Zero Knowledge Proofs

Secret Sharing

Conclusion

Interactive Zero Knowledge Proofs

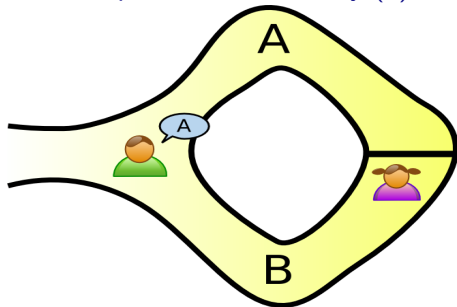
An Example: The Cave Story (2)



First, Victor waits outside while Peggy chooses a path.

Interactive Zero Knowledge Proofs

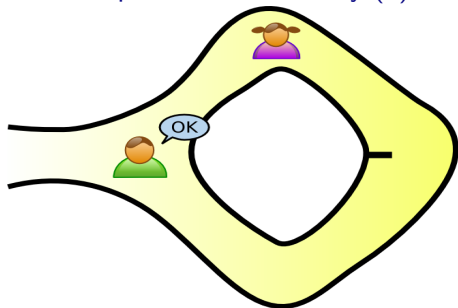
An Example: The Cave Story (3)



Then Victor enters and shouts the name of a path.

Interactive Zero Knowledge Proofs

An Example: The Cave Story (4)



At last, Peggy returns along the desired path (using the secret if necessary).

Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

Logical Attacks

Interactive Zero Knowledge Proofs

Secret Sharing

Conclusion

Secret Sharing

- ▶ How keep nuclear code secret in British Army?

Secret Sharing

- ▶ How keep nuclear code secret in British Army?
- ▶ Burn it, but do not preseve integrity

How to Share a Secret Code I



1234567



How to Share a Secret Code I

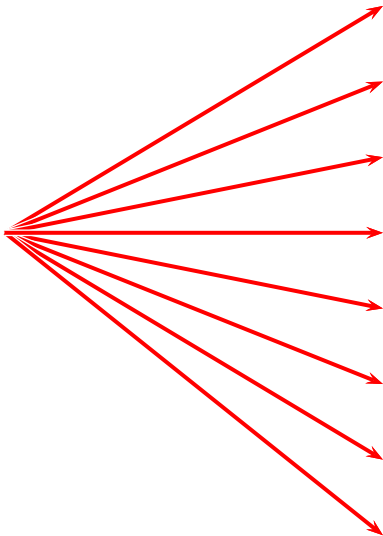


1234567



Problem of Integrity and Confidentiality

How to Share a Secret Code II



1234567



1234567



1234567

1234567



1234567

1234567

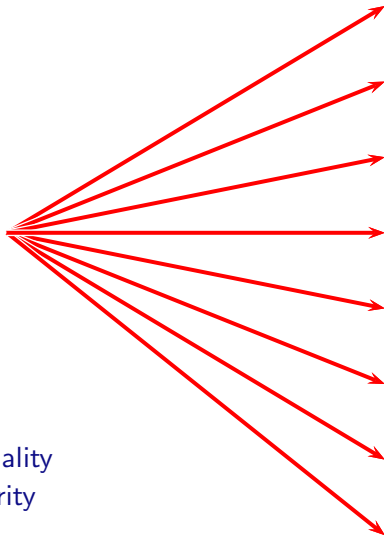


1234567



1234⁴⁶567⁵²

How to Share a Secret Code II



1234567



1234567



1234567

1234567



1234567



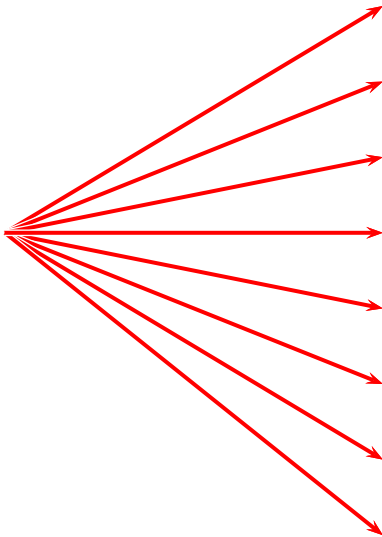
1234567

1234567

1234⁴⁶567⁵²

Problem of Confidentiality
No problem of Integrity

How to Share a Secret Code II



23572



11567



734567

534567



934567

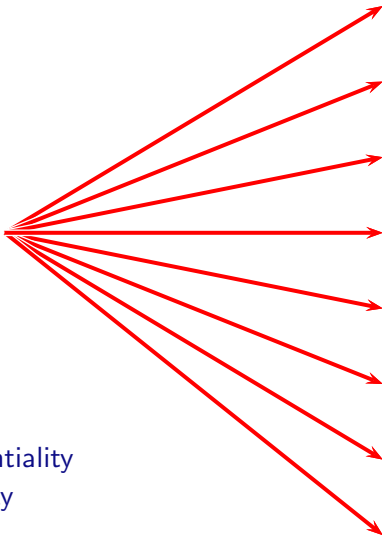


563317

114567

455567^{17/52}

How to Share a Secret Code II



23572



11567



734567

534567



934567

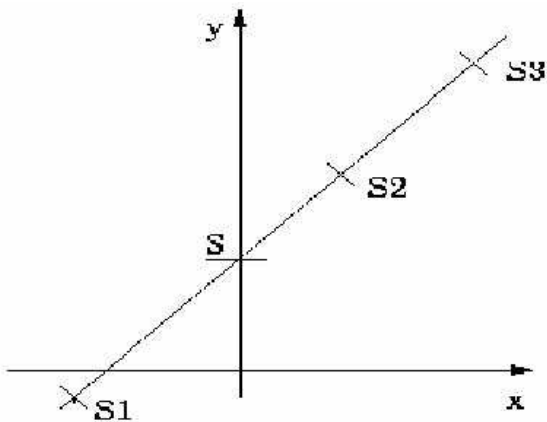


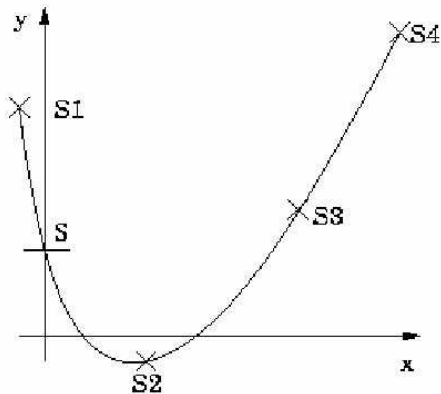
563317

114567

455567^{47/52}

No Problem of Confidentiality
Problem of Integrity

$(2,5)$ 

$(3,5)$ 

Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

Logical Attacks

Interactive Zero Knowledge Proofs

Secret Sharing

Conclusion

Summary

Today

- ▶ Motivation
- ▶ History of Cryptography
- ▶ Security notions
- ▶ Logical attacks
- ▶ Zero - knowledge
- ▶ Secret Sharing

Thank you for your attention



Questions ?

pascal.lafourcade@imag.fr