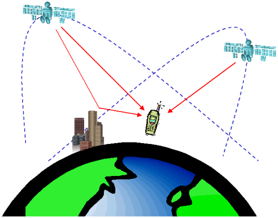
Security and Cryptography just by images

Pascal Lafourcade

2010

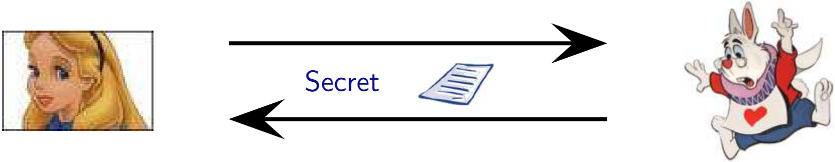
pascal.lafourcade@imag.fr

Applications



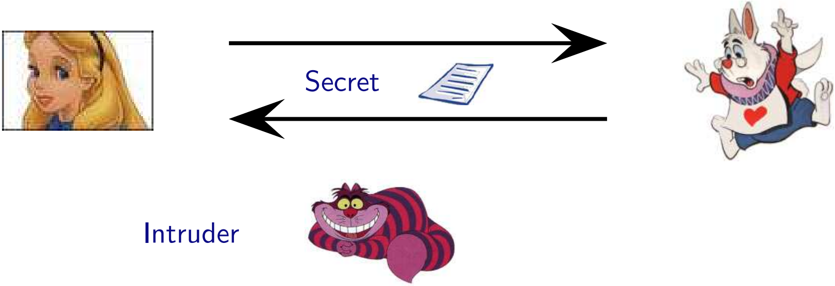
Secrecy or Confidentiality

Alice communicates with the White rabbit via a network.



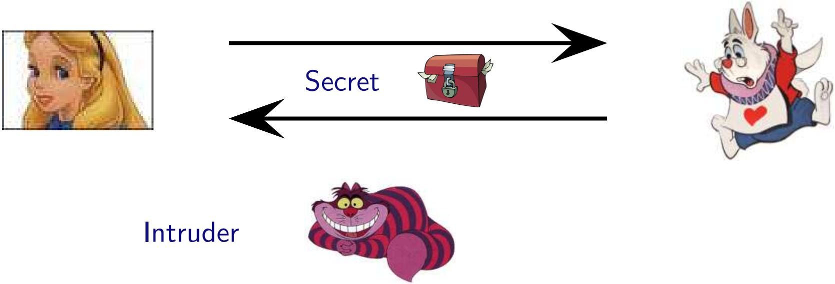
Secrecy or Confidentiality

Alice communicates with the White rabbit via a network.



Secrecy or Confidentiality

Alice communicates with the White rabbit via a network.



Authentication

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

Mechanisms for Authentication

1. 

Mechanisms for Authentication

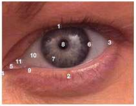
1. 

2. 

Mechanisms for Authentication

1. 

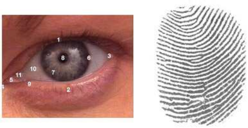
2. 

3.  

Mechanisms for Authentication

1. 

2. 

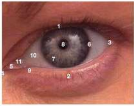
3. 

4. 

Mechanisms for Authentication

1. 

2. 

3.  

4. 

Strong authentication combination of factors.

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

Outline

Motivations

Two Examples

Outline

Motivations

Two Examples

History of Cryptography

Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

Logical Attacks

Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

Logical Attacks

Interactive Zero Knowledge Proofs

Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

Logical Attacks

Interactive Zero Knowledge Proofs

Secret Sharing

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

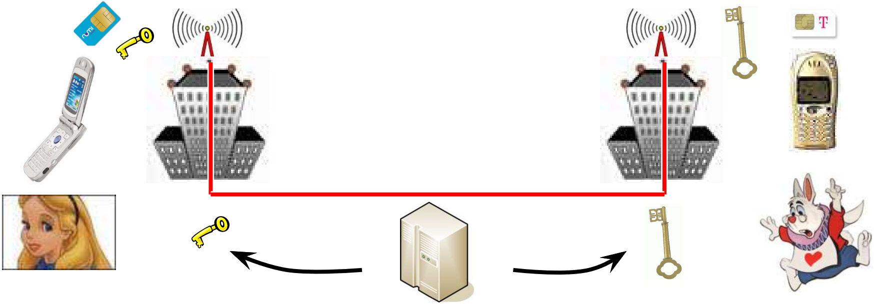
Logical Attacks

Interactive Zero Knowledge Proofs

Secret Sharing

Conclusion

Symetric 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 uncrypted.
3. Message is encrypted by the antenna with the second key.
4. Second mobile uncrypted 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.

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

$H(\mathit{Alice}) \;=\; \neq \; H(\mathit{Bob})$

$\mathit{marion} \;\rightarrow$

$\mathit{marine} \;\nrightarrow \qquad \leftarrow \; \mathit{laurence}$

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

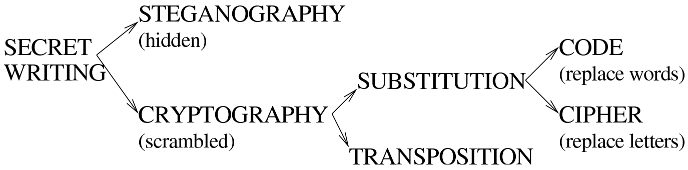
Logical Attacks

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 =

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

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

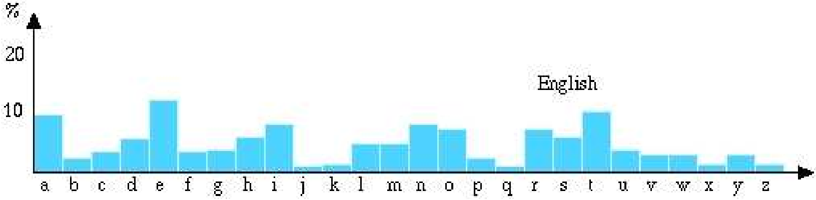
Substitution cipher examples

- 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

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

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

Example

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

Improvement: Homophonic substitution ciphers

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

$H(a) = \{00, 10\}$, 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

- $C =$ AduaenttlydhatoiekounletmtoihahvsekeeeleeyqonouV

Example: transposition ciphers

- C = Aduaenttlydhatoiekounletmtoihahvsekeeeleeyqonouv

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, ..., 50.

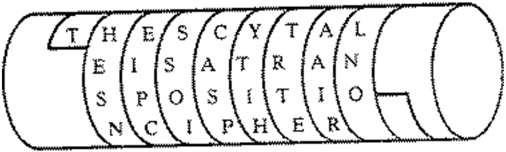
Example: transposition ciphers

- $C =$ Aduaenttlydhatoiekounletmtoihahvsekeeeleeyqonouv

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, ..., 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
  $\rightsquigarrow$ invention of cipher machines.

One-time pad (Vernam cipher)

One-time pad (Vernam cipher)

- Example: $\begin{array}{ccc} m & = & 010111 \\ k & = & 110010 \\ \hline c & = & 100101 \end{array}$
- Unconditional (information theoretic) security, if key isn't reused!
- Problem?

One-time pad (Vernam cipher)

- Example: $\begin{array}{rcl} m & = & 010111 \\ k & = & 110010 \\ \hline c & = & 100101 \end{array}$
- 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

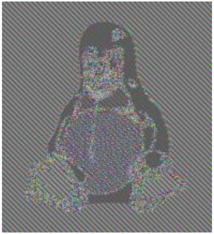
Interactive Zero Knowledge Proofs

Secret Sharing

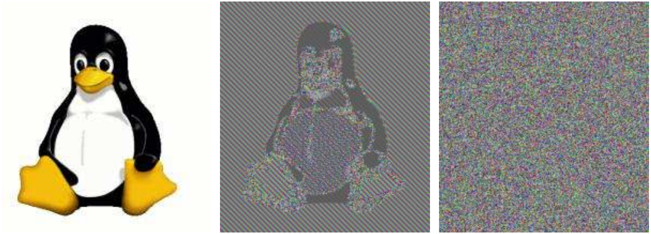
Conclusion

ECB vs Others

ECB vs Others

ECB vs Others



One-Wayness (OW)

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

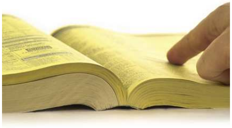
One-Wayness (OW)

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

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

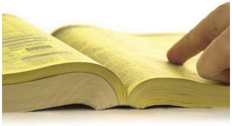
One Way Function

- Applying f is easy
- Computing f^{-1} is difficult



One Way Function

- Applying f is easy
- Computing f^{-1} is difficult



Factorization

- $p, q \mapsto n = p.q$ easy (quadratic)
- $n = p.q \mapsto p, q$ difficult

Known Results (1/2)

Fermat's Little Theorem

If a is not divisible by a prime p then p divides $a^{p-1} - 1$

Euclid Theorem

If a prime p divides the product bc then p divides either b or c.

Known Results (2/2)

Chinese Remainder Theorem

Suppose $n_1, n_2, \ldots, n_k$ are positive integers which are pairwise coprime. Then, for any given set of integers $a_1, a_2, \ldots, a_k$, there exists an integer x solving the system of simultaneous congruences

$$x \equiv a_1 \pmod{n_1} \tag{1}$$
$$x \equiv a_2 \pmod{n_2} \tag{2}$$
$$\vdots \tag{3}$$
$$x \equiv a_k \pmod{n_k} \tag{4}$$

Furthermore, all solutions x to this system are congruent modulo the product $N = n_1 n_2 \ldots n_k$.

Hence $x \equiv y \pmod{n_i}$ for all $1 \leq i \leq k$, if and only if $x \equiv y \pmod{N}$.

RSA 1977 (Rivest, Shamir & Adelman)

Public key: e, n

Secret key: p, q

where $n = pq$, p and q primes.

- Encryption $c = m^e \mod n$ easy
- Decryption $m = c^d \mod n$ difficult
  where $d = e^{-1} \mod \varphi(n) = (p-1)(q-1)$

RSA, Key generation

- Let p and q two primes
- Let $n = pq$
- Compute Euler function $\varphi(n) = (p-1)(q-1)$
- Select e prime with $\varphi(n)$

RSA, Key generation

- Let p and q two primes
- Let $n = pq$
- Compute Euler function $\varphi(n) = (p-1)(q-1)$
- Select e prime with $\varphi(n)$

Since e prime with $\varphi(n)$ using Bézout Theorem:

$$\exists d, ed \equiv 1 \pmod{\varphi(n)}$$

RSA, Key generation

- Let p and q two primes
- Let $n = pq$
- Compute Euler function $\varphi(n) = (p-1)(q-1)$
- Select e prime with $\varphi(n)$

Since e prime with $\varphi(n)$ using Bézout Theorem:

$$\exists d, ed \equiv 1 \pmod{\varphi(n)}$$

RSA parameters

- Public key $= (n, e)$
- Private key $= (n, d)$

RSA, Decryption (1/3)

If $d = e^{-1} \mod \varphi(n) = (p-1)(q-1)$, why $m = c^d \mod n$

RSA, Decryption (1/3)

If $d = e^{-1} \mod \varphi(n) = (p-1)(q-1)$, why $m = c^d \mod n$

$$C^d \pmod{n} \equiv (M^e)^d \pmod{n} \equiv M^{ed} \pmod{n}$$

RSA, Decryption (1/3)

If $d = e^{-1} \mod \varphi(n) = (p-1)(q-1)$, why $m = c^d \mod n$

$$C^d \pmod n \equiv (M^e)^d \pmod n \equiv M^{ed} \pmod n$$

by definition $ed \equiv 1 \pmod{\varphi(n)}$ hence

RSA, Decryption (1/3)

If $d = e^{-1} \mod \varphi(n) = (p-1)(q-1)$, why $m = c^d \mod n$

$$C^d \pmod{n} \equiv (M^e)^d \pmod{n} \equiv M^{ed} \pmod{n}$$

by definition $ed \equiv 1 \pmod{\varphi(n)}$ hence

$$ed = 1 + k\varphi(n) = 1 + k(p-1)(q-1), k \in \mathbb{N}$$

We have to show using Fermat's Little Theorem: $\forall M \in \mathbb{N}$,

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{p}$$

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{q}$$

RSA, Decryption (2/3)

- If M is prime with p then, using Fermat's Little Theorem,

$$M^{p-1} \equiv 1 \pmod{p}$$

$$M^{k(p-1)(q-1)} \equiv 1 \pmod{p}$$

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{p}$$

RSA, Decryption (2/3)

- If M is prime with p then, using Fermat's Little Theorem,

$$M^{p-1} \equiv 1 \pmod{p}$$

$$M^{k(p-1)(q-1)} \equiv 1 \pmod{p}$$

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{p}$$

- Otherwise p divides M, but p is prime, it means that

$$l.p \equiv M \equiv 0 \equiv M^{1+k(p-1)(q-1)} \pmod{p}$$

Same for q.

RSA, Decryption (1/3)

$$\forall M \in \mathbb{N},$$
$$M^{1+k(p-1)(q-1)} \equiv M \pmod{p}$$
$$M^{1+k(p-1)(q-1)} \equiv M \pmod{q}$$

RSA, Decryption (1/3)

$$\forall M \in \mathbb{N},$$
$$M^{1+k(p-1)(q-1)} \equiv M \pmod{p}$$
$$M^{1+k(p-1)(q-1)} \equiv M \pmod{q}$$

p and q divide $M^{1+k(p-1)(q-1)} - M$. Moreover p and q are distinct primes, using Chinese Remainder Theorem, we conclude $n = pq$ divides $M^{1+k(p-1)(q-1)} - M$

RSA, Decryption (1/3)

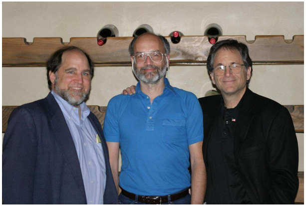
$$\forall M \in \mathbb{N},$$
$$M^{1+k(p-1)(q-1)} \equiv M \pmod{p}$$
$$M^{1+k(p-1)(q-1)} \equiv M \pmod{q}$$

p and q divide $M^{1+k(p-1)(q-1)} - M$. Moreover p and q are distinct primes, using Chinese Remainder Theorem, we conclude $n = pq$ divides $M^{1+k(p-1)(q-1)} - M$

$$C^d \equiv M^{ed} \equiv M^{1+k(p-1)(q-1)} \equiv M \pmod{n}$$

RSA : Rivest, Shamir & Adelman

RSA : Rivest, Shamir & Adelman



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.

ElGamal is IND

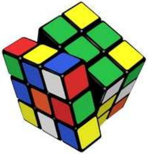
- $G = (\langle g \rangle, *)$ finite cyclic group of prime order q.
- x: private key.
- $y = g^x$: public key.

$$\mathcal{E}(m; r) = (g^r, y^r m) \to (c, d)$$

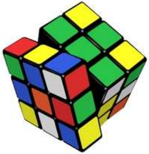
$$\mathcal{D}(c, d) = \frac{d}{c^x}$$

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

$\Downarrow$

Indistinguishability

$\Downarrow$

One-Wayness

Key Privacy or Key Anonymity

Key Privacy or Key Anonymity





Key Privacy or Key Anonymity





SOLUTION

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

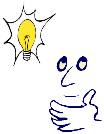
Computational Model
Cryptanalysis

Symbolic Model
Logical Attack

Perfect Encryption hypothesis

Needham-Schroeder Public Key Protocol (1978)

"Man in the middle attack" [Lowe'96]



Simple Example

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

Simple Example

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

Simple Example

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

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

Day After

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

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

Simple Example

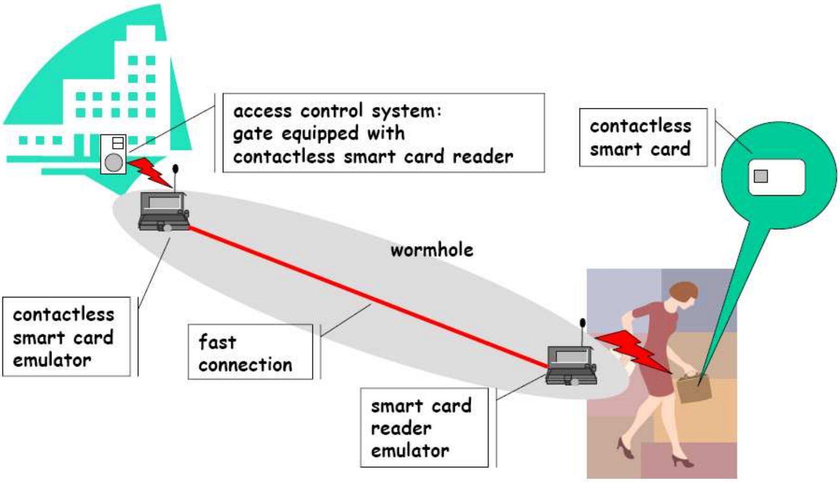
 $\xrightarrow{\{12h10\}_{K_B}}$  $\xrightarrow{\{12h10\}_{K_B}}$ 

Day After

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

This kind of attack is valid for all encryptions

Authentication Problem: Wormhole Attack



Example: Needham-Schroeder Protocol 1978

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

Example: Needham-Schroeder Protocol 1978

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

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

Example: Needham-Schroeder Protocol 1978

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

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

$$\longrightarrow \{N_B\}_{K_B} \longrightarrow$$

Example: Needham-Schroeder Protocol 1978

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

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

$$\longrightarrow \quad \{N_B\}_{K_B} \quad \longrightarrow$$

Question

- Is N_B a shared secret between A et B?

Example: Needham-Schroeder Protocol 1978

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

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

$$\longrightarrow \{N_B\}_{K_B} \longrightarrow$$

Question

- Is N_B a shared secret between A et B?

Answer

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

Lowe Attack on the Needham-Schroeder

so-called “Man in the middle attack”

Agent A

Intruder I

Agent B

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

Lowe Attack on the Needham-Schroeder

so-called “Man in the middle attack”

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

Agent A

Intruder I

Agent B

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

Lowe Attack on the Needham-Schroeder

so-called "Man in the middle attack"

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

$\xrightarrow{\{A, N_a\}_{K_B}}$

Agent A

Intruder I

Agent B

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

Lowe Attack on the Needham-Schroeder

so-called "Man in the middle attack"

Agent A Intruder I Agent B

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

Lowe Attack on the Needham-Schroeder

so-called “Man in the middle attack”

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

$\longleftarrow \{N_a, N_b\}_{K_A}$

$\{A, N_a\}_{K_B} \longrightarrow$

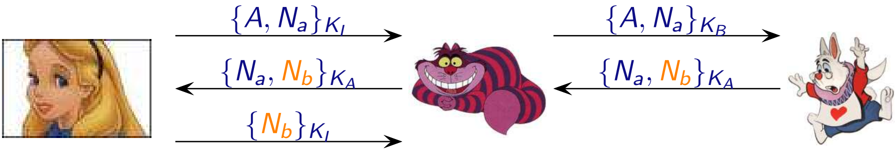
$\longleftarrow \{N_a, N_b\}_{K_A}$

Agent A | Intruder I | Agent B

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

Lowe Attack on the Needham-Schroeder

so-called “Man in the middle attack”

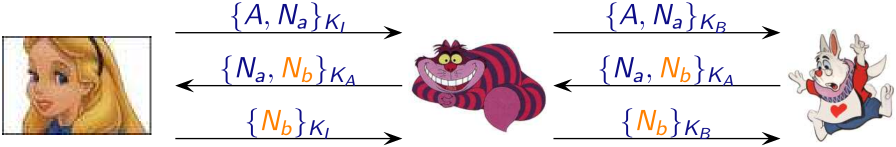


Agent A | Intruder I | Agent B

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

Lowe Attack on the Needham-Schroeder

so-called "Man in the middle attack"



Agent A Intruder I Agent B

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

Needham-Schroeder corrected by Lowe 1995

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

Needham-Schroeder corrected by Lowe 1995

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

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

Needham-Schroeder corrected by Lowe 1995

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

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

$\longrightarrow \{N_B\}_{K_B} \longrightarrow$

Needham-Schroeder corrected by Lowe 1995

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

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

$\longrightarrow \{N_B\}_{K_B} \longrightarrow$

Question

- This time the protocol is secure?

Outline

Motivations

Two Examples

History of Cryptography

Cryptographic Security Intuitions

Logical Attacks

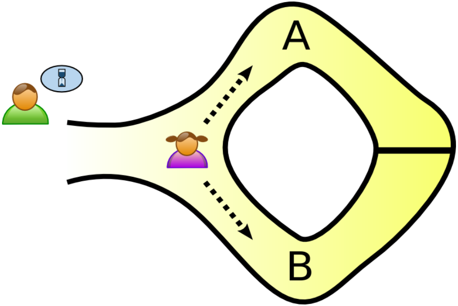
Interactive Zero Knowledge Proofs

Secret Sharing

Conclusion

Interactive Zero Knowledge Proofs

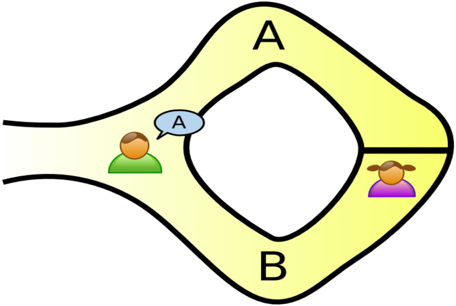
An Example: The Cave Story (2)



First, Victor waits outside while Peggy chooses a path.

Interactive Zero Knowledge Proofs

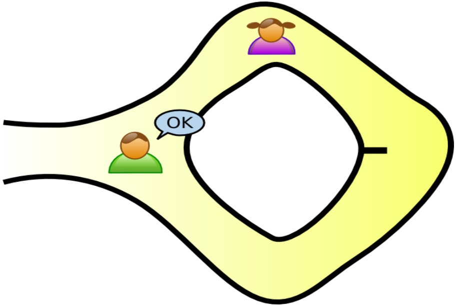
An Example: The Cave Story (3)



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

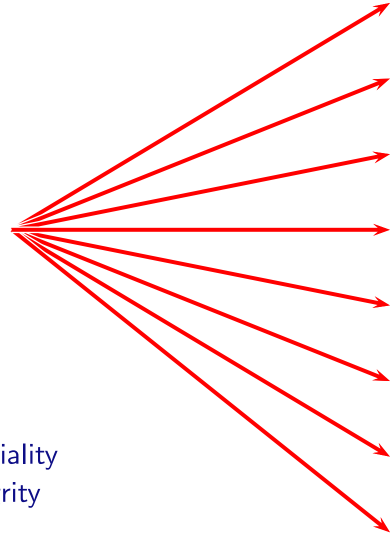
How to Share a Secret Code I

1234567

Problem of Integrity and Confidentiality

How to Share a Secret Code II

How to Share a Secret Code II




1234567


1234567


1234567

1234567


1234567


1234567

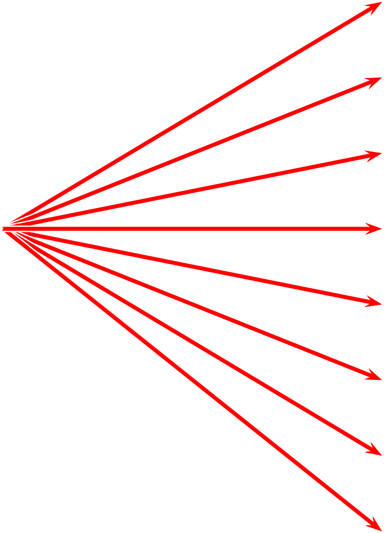
1234567


1234567

Problem of Confidentiality

No problem of Integrity

How to Share a Secret Code II



23572

11567

734567

534567

934567

563317

114567

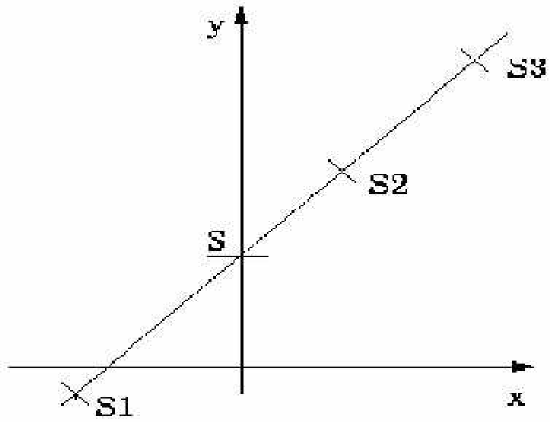
455567

How to Share a Secret Code II

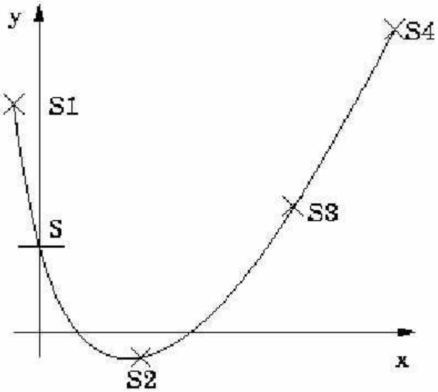
No Problem of Confidentiality

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
- Securities notions
- Logical attacks
- Zero - knowledge
- Secret Sharing

Thank you for your attention

Questions ?

pascal.lafourcade@imag.fr