

# Advanced Cryptography 1st Semester 2008-2009

## Symmetric Encryption

**Pascal Lafourcade**

*Université Joseph Fourier, Verimag*

Master: October 13th 2008

# Last Time (I)

## Security Notions

- Cyclic Groups
- Hard Problems
- One-way
- IND-CPA, IND-CCA1, IND-CCA2
- NM-CPA, NM-CCA1, NM-CCA2
- Examples
  - RSA
  - ElGamal
- IND-CCA2  $\Rightarrow$  NM-CCA2
- NM-CCA1  $\not\Rightarrow$  NM-CPA

Remarks, questions, comments ?

## Last Time (II)

### Exercises done

- 1) Indistinguishability
- 2) IND-XXX
- 3) Random encryption is useful
- 4)  $DDH \leq CDH \leq DL$

## Outline of Today: **Security Notions**

- 1 Recall
- 2 Block cipher modes
  - ECB
  - CBC
  - CFB
  - OFB
- 3 Attack on ECB
- 4 Hybrid Encryption
- 5 OAEP
- 6 Logical Attacks
- 7 Needham Schroeder
- 8 Conclusion

# Outline

- 1 Recall
- 2 Block cipher modes
  - ECB
  - CBC
  - CFB
  - OFB
- 3 Attack on ECB
- 4 Hybrid Encryption
- 5 OAEP
- 6 Logical Attacks
- 7 Needham Schroeder
- 8 Conclusion

# Symmetric key and public key encryption

- Symmetric key encryption



- Public key encryption



## Summary of IND-XXX Games

Given  $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ ,  $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$  of polynomial-time probabilistic algorithms.  $\text{IND}_{\text{XXX}}^b(\mathcal{A})$  follows:

- Generate  $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$ .
- $(s, m_0, m_1) \xleftarrow{R} \mathcal{A}_1^{\mathcal{O}_1}(\eta, pk)$
- $b' \xleftarrow{R} \mathcal{A}_2^{\mathcal{O}_2}(\eta, pk, s, \mathcal{E}(pk, m_b))$
- return  $b'$ .

$$\text{ADV}_{\mathcal{S}, \mathcal{A}}^{\text{IND}_{\text{XXX}}}(\eta) =$$

$$\Pr[b' \xleftarrow{R} \text{IND}_{\text{XXX}}^1(\mathcal{A}) : b' = 1] - \Pr[b' \xleftarrow{R} \text{IND}_{\text{XXX}}^0(\mathcal{A}) : b' = 1]$$

### IND-CPA, IND-CCA1, IND-CCA2

IND-CPA:  $\mathcal{O}_1 = \mathcal{O}_2 = \emptyset$  Chosen Plain text Attack

IND-CCA1:  $\mathcal{O}_1 = \{\mathcal{D}\}$ ,  $\mathcal{O}_2 = \emptyset$  Non-adaptive Chosen Cipher text Attack

IND-CCA2:  $\mathcal{O}_1 = \mathcal{O}_2 = \{\mathcal{D}\}$  Adaptive Chosen Cipher text Attack.

## The NM-XXX Games

Given  $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ . An adversary  $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$  of polynomial-time probabilistic algorithms,  $m, m', m^* \in M$ . Let  $NM_{XXX}^b(\mathcal{A})$ :

- Generate  $(pk, sk) \xleftarrow{R} \mathcal{K}(\eta)$ .
- $(s, M) \xleftarrow{R} \mathcal{A}_1^{\mathcal{O}_1}(\eta, pk), m_0, m_1, \leftarrow M$
- $(R, C') \xleftarrow{R} \mathcal{A}_2^{\mathcal{O}_2}(\eta, pk, s, M, \mathcal{E}(pk, m_b)), M' \leftarrow \mathcal{D}(C')$
- return  $R(m_b, M')$

Then, we define the advantage against the IND-CCA2 game by:

$$\begin{aligned} \text{ADV}_{\mathcal{S}, \mathcal{A}}^{NM_{XXX}}(\eta) &= \Pr[R(m, M') \xleftarrow{R} NM_{XXX}^1(\mathcal{A}) : R(m, M') = 1] \\ &\quad - \Pr[R(m, M^*) \xleftarrow{R} NM_{XXX}^0(\mathcal{A}) : R(m, M^*) = 1] \end{aligned}$$

NM-CPA:  $\mathcal{O}_1 = \mathcal{O}_2 = \emptyset$  Chosen Plain text Attack

NM-CCA1:  $\mathcal{O}_1 = \{\mathcal{D}\}, \mathcal{O}_2 = \emptyset$  Non-adaptive Chosen Cipher text Attack

NM-CCA2:  $\mathcal{O}_1 = \mathcal{O}_2 = \{\mathcal{D}\}$  Adaptive Chosen Cipher text Attack.

# Outline

- 1 Recall
- 2 Block cipher modes
  - ECB
  - CBC
  - CFB
  - OFB
- 3 Attack on ECB
- 4 Hybrid Encryption
- 5 OAEP
- 6 Logical Attacks
- 7 Needham Schroeder
- 8 Conclusion

## Electronic Book Code (ECB)

Each block of the same length is encrypted separately using the same key  $K$ . In this mode, only the block in which the flipped bit is contained is changed. Other blocks are not affected.

# ECB Encryption Algorithm

**algorithm**  $E_K(M)$

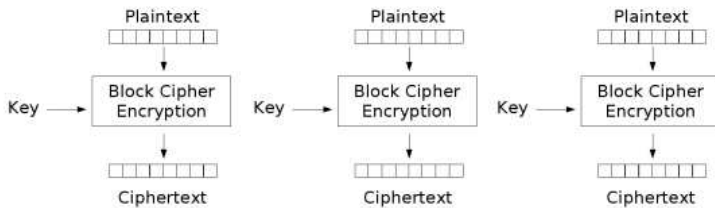
if  $(|M| \bmod n \neq 0 \text{ or } |M| = 0)$  then return FAIL

Break  $M$  into  $n$ -bit blocks  $M[1] \dots M[m]$

for  $i = 1$  to  $m$  do  $C[i] = E_K(M[i])$

$C = C[1] \dots C[m]$

return  $C$



Electronic Codebook (ECB) mode encryption

## ECB Decryption Algorithm

**algorithm**  $D_K(C)$

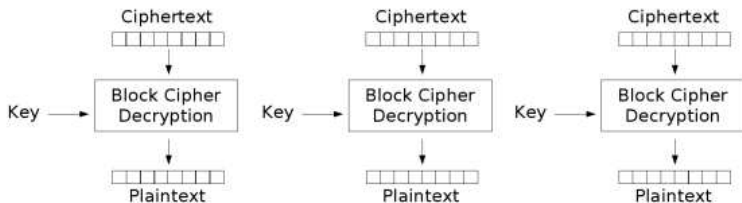
if  $(|C| \bmod n \neq 0 \text{ or } |C| = 0)$  then return FAIL

Break  $C$  into  $n$ -bit blocks  $C[1] \dots C[m]$

for  $i = 1$  to  $m$  do  $M[i] = D_K(C[i])$

$M = M[1] \dots M[m]$

return  $M$



Electronic Codebook (ECB) mode decryption

## Cipher-block chaining (CBC)

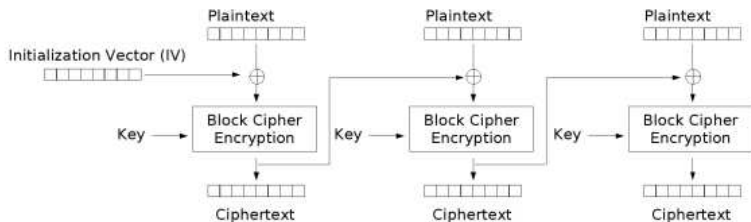
If the first block has index 1, the mathematical formula for CBC encryption is

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

while the mathematical formula for CBC decryption is

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV$$

CBC has been the most commonly used mode of operation.



Cipher Block Chaining (CBC) mode encryption



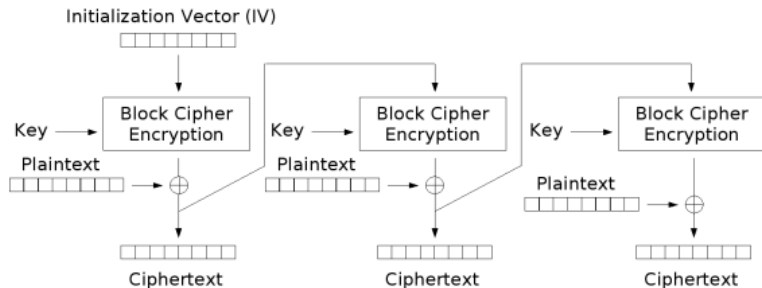
## The cipher feedback (CFB)

A close relative of CBC:

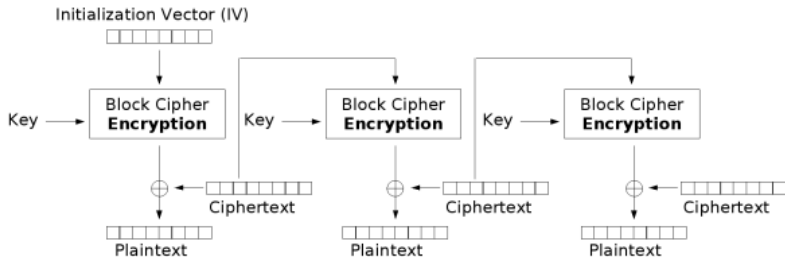
$$C_i = E_K(C_{i-1}) \oplus P_i$$

$$P_i = E_K(C_{i-1}) \oplus C_i$$

$$C_0 = IV$$



Cipher Feedback (CFB) mode encryption



Cipher Feedback (CFB) mode decryption

## Output feedback (OFB)

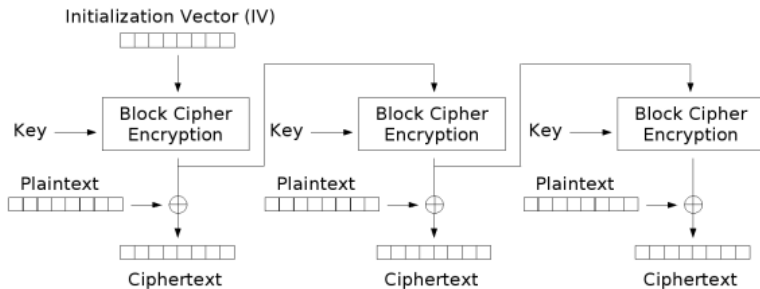
Because of the symmetry of the XOR operation, encryption and decryption are exactly the same:

$$C_i = P_i \oplus O_i$$

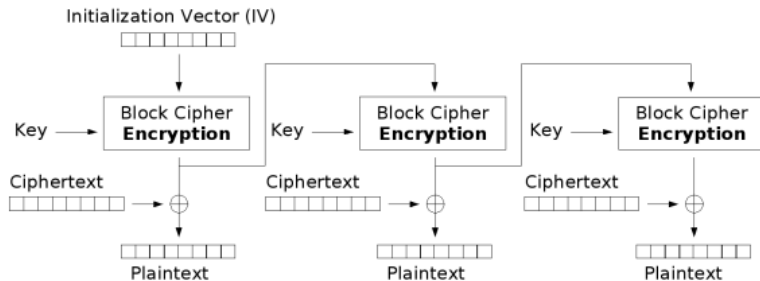
$$P_i = C_i \oplus O_i$$

$$O_i = E_K(O_{i-1})$$

$$O_0 = IV$$

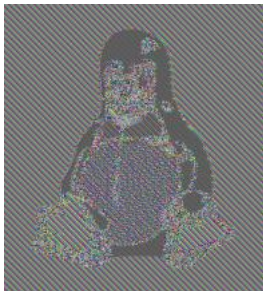


Output Feedback (OFB) mode encryption



Output Feedback (OFB) mode decryption

## ECB vs Others



# Outline

- 1 Recall
- 2 Block cipher modes
  - ECB
  - CBC
  - CFB
  - OFB
- 3 Attack on ECB**
- 4 Hybrid Encryption
- 5 OAEP
- 6 Logical Attacks
- 7 Needham Schroeder
- 8 Conclusion

## ECB Attack

Let us fix a block cipher  $\mathcal{E} : \mathcal{K} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ . and  $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$  an ECB symmetric encryption scheme, where the size of each block is  $n$ .

We build an adversary  $A$  with a high IND-CPA advantage.

$$\mathcal{E}_K(LR(m_l, m_r, b)) = \begin{cases} \mathcal{E}_K(m_l) & \text{if } b = 1 \\ \mathcal{E}_K(m_r) & \text{if } b = 0 \end{cases}$$

## Adversary A

**Adversary**  $A^{\mathcal{E}_K(LR(\cdot, \cdot, b))}$

$M_0 \leftarrow 0^n || 1^n;$

$M_1 \leftarrow 0^{2n};$

$C[1]C[2] \leftarrow \mathcal{E}_K(LR(M_0, M_1, b))$

If  $C[1] = C[2]$  then return 1 else return 0

$X[i]$  denotes the  $i$ -th block of a string  $X$ , a block being a sequence of  $n$  bits.

# Proof

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 0}(A) = 1] = 0$$

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 1}(A) = 1] = 1$$

Why?

# Proof

$$\Pr[\text{Exp}_{\mathcal{SE}}^{\text{IND-CPA } 0}(A) = 1] = 0$$

$$\Pr[\text{Exp}_{\mathcal{SE}}^{\text{IND-CPA } 1}(A) = 1] = 1$$

## Why?

- If  $b = 1$ , then the oracle returns  $C[1]C[2] = \mathcal{E}_K(0^n) || \mathcal{E}_K(0^n)$ , so  $C[1] = C[2]$  and  $A$  returns 1.

# Proof

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 0}(A) = 1] = 0$$

$$\Pr[\text{Exp}_{S\mathcal{E}}^{\text{IND-CPA } 1}(A) = 1] = 1$$

## Why?

- If  $b = 1$ , then the oracle returns  $C[1]C[2] = \mathcal{E}_K(0^n) \parallel \mathcal{E}_K(0^n)$ , so  $C[1] = C[2]$  and  $A$  returns 1.
- if  $b = 0$ , the oracle returns  $C[1]C[2] = \mathcal{E}_K(0^n) \parallel \mathcal{E}_K(1^n)$ . Hence  $C[1] \neq C[2]$ . So  $A$  returns 0 in this case.

# Proof

$$\Pr[\text{Exp}_{\mathcal{SE}}^{\text{IND-CPA } 0}(A) = 1] = 0$$

$$\Pr[\text{Exp}_{\mathcal{SE}}^{\text{IND-CPA } 1}(A) = 1] = 1$$

## Why?

- If  $b = 1$ , then the oracle returns  $C[1]C[2] = \mathcal{E}_K(0^n) || \mathcal{E}_K(0^n)$ , so  $C[1] = C[2]$  and  $A$  returns 1.
- if  $b = 0$ , the oracle returns  $C[1]C[2] = \mathcal{E}_K(0^n) || \mathcal{E}_K(1^n)$ . Hence  $C[1] \neq C[2]$ . So  $A$  returns 0 in this case.

$$\text{Adv}_{\mathcal{SE}}^{\text{IND-CPA}}(A) = 1 - 0 = 1$$

This means that the ECB encryption scheme is insecure.

# Exercise

- 1 Find an attack on CBC with counter IV.
- 2 Prove that CBC with random IV is not IND-CCA1 secure.
- 3 Notice that CBC with random IV is IND-CPA secure.

# Outline

- 1 Recall
- 2 Block cipher modes
  - ECB
  - CBC
  - CFB
  - OFB
- 3 Attack on ECB
- 4 Hybrid Encryption**
- 5 OAEP
- 6 Logical Attacks
- 7 Needham Schroeder
- 8 Conclusion

## Idea and Motivations

### Idea

$A\mathcal{E} = (\mathcal{K}^a, \mathcal{E}^a, \mathcal{D}^a)$  an asymmetric encryption scheme  $(pk, sk)$ .  
 $S\mathcal{E} = (\mathcal{K}^s, \mathcal{E}^s, \mathcal{D}^s)$  a symmetric encryption scheme  $K$ .

We define  $\overline{\mathcal{E}}_{pk}(M)$  using  $\mathcal{E}_K^s(M)$  and  $\mathcal{E}_{pk}^a(K)$

### Motivation

Costly operation (asymmetric encryption) is applied on a message of fixed size, and after efficient algorithm are used to encrypt the data.

## Encryption Algorithm

**Algorithm**  $\overline{\mathcal{E}}_{pk}(M)$

$K \leftarrow K^s;$

$C^s \leftarrow \mathcal{E}_K^s(M);$

$C^a \leftarrow \mathcal{E}_{pk}^a(K);$

$C \leftarrow (C^a, C^s);$

Return  $C$

## Decryption Algorithm

**Algorithm**  $\overline{\mathcal{D}}_{sk}(C)$   
Parse  $C$  as  $(C^a, C^s)$ ;  
 $K \leftarrow \mathcal{D}_{sk}^a(C^a)$ ;  
 $M \leftarrow \mathcal{D}_K^s(C^s)$ ;  
Return  $M$

# Security

## Property

If  $A\mathcal{E}$  and  $S\mathcal{E}$  are each secure against chosen-plain-text attack, then  $\overline{A\mathcal{E}}$  the hybrid encryption is also secure against chosen-plain-text attack.

Let  $B$  be an IND-CPA adversary attacking  $\overline{A\mathcal{E}}$ . Then there exist IND-CPA adversaries  $A_{00,01}, A_{11,10}$  attacking  $A\mathcal{E}$ , and an adversary  $A$  attacking  $S\mathcal{E}$ , such that:

$$\begin{aligned} Adv_{\overline{A\mathcal{E}}}^{IND-CPA}(B) &\leq Adv_{A\mathcal{E}}^{IND-CPA}(A_{00,01}) + Adv_{A\mathcal{E}}^{IND-CPA}(A_{11,10}) \\ &\quad + Adv_{S\mathcal{E}}^{IND-CPA}(A) \end{aligned}$$

## Idea of the Proof

$$P(\alpha, \beta) = \Pr[\text{Exp}_{\mathcal{AE}}^{\alpha\beta}(B) = 1]$$

$$P(1, 0) = \Pr[\text{Exp}_{\mathcal{AE}}^{\text{IND-CPA-1}}(B) = 1]$$

$$P(0, 0) = \Pr[\text{Exp}_{\mathcal{AE}}^{\text{IND-CPA-0}}(B) = 1]$$

$$\text{Adv}_{\mathcal{AE}}^{\text{IND-CPA}}(B) = P(1, 0) - P(0, 0)$$

## General Scheme of the Proof

$$P(1, 0) - P(0, 0) = \\ [P(1, 0) - P(1, 1)] + [P(1, 1) - P(0, 1)] + [P(0, 1) - P(0, 0)]$$

$$P(1, 0) - P(1, 1) \leq Adv_{\mathcal{AE}}^{IND-CPA}(A_{11,10})$$

$$P(1, 1) - P(0, 1) \leq Adv_{\mathcal{SE}}^{IND-CPA}(A)$$

$$P(0, 1) - P(0, 0) \leq Adv_{\mathcal{AE}}^{IND-CPA}(A_{00,01})$$

# Outline

- 1 Recall
- 2 Block cipher modes
  - ECB
  - CBC
  - CFB
  - OFB
- 3 Attack on ECB
- 4 Hybrid Encryption
- 5 OAEP**
- 6 Logical Attacks
- 7 Needham Schroeder
- 8 Conclusion

## Optimal Asymmetric Encryption Padding (OAEP)

The OAEP cryptosystem  $(\mathcal{K}, \mathcal{E}, \mathcal{D})$  obtained from a permutation  $f$ , whose inverse is denoted by  $g$ . And two hash functions:

$$G : \{0, 1\}^{k_0} \rightarrow \{0, 1\}^{k-k_0}$$

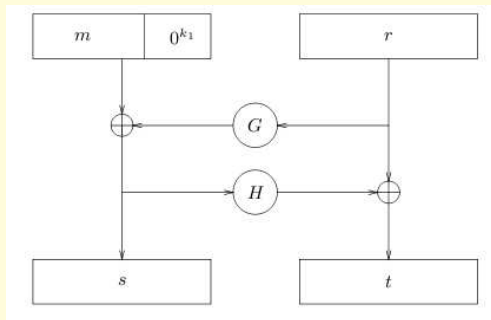
$$H : \{0, 1\}^{k-k_0} \rightarrow \{0, 1\}^{k_0}$$

$\mathcal{K}(1^k)$ : specifies an instance of the function  $f$ , and of its inverse  $g$ .  
The public key  $pk$  is therefore  $f$  and the private key  $sk$  is  $g$ .

# OAEP: Encryption

$\mathcal{E}_{pk}(m, r) = c$  with  $m \in \{0, 1\}^n$ , and  $r \leftarrow \{0, 1\}^{k_0}$

$$s = (m || 0^{k_1}) \oplus G(r), t = r \oplus H(s)$$



$$c = f(s, t)$$

## OAEP: Decryption

 $\mathcal{D}_{sk}(c)$ 

$$g(c) = (s, t)$$

$$r = t \oplus H(s)$$

$$M = s \oplus G(r)$$

If  $[M]_{k_1} = 0^{k_1}$ , the algorithm returns  $[M]^n$ , otherwise it returns "Reject"

- $[M]_{k_1}$  denotes the  $k_1$  least significant bits of  $M$
- $[M]^n$  denotes the  $n$  most significant bits of  $M$

## Results and References

OAEP was first proved IND-CPA then IND-CCA1 and finally IND-CCA2 secure under some assumptions.

- 1 M. Bellare, P. Rogaway. “Optimal Asymmetric Encryption – How to encrypt with RSA”. Extended abstract in Advances in Cryptology - Eurocrypt '94 Proceedings, LNCS Vol. 950, A. Springer-Verlag, 1995.
- 2 Victor Shoup. “OAEP Reconsidered”. IBM Zurich Research Lab, September 18, 2001.
- 3 Eiichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval, and Jacques Stern. “RSA– OAEP is secure under the RSA assumption”. In J. Kilian, ed., Advances in Cryptology – CRYPTO 2001, vol. 2139 of LNCS, SpringerVerlag, 2001.
- 4 P. Paillier and J. Villar, “Trading One-Wayness against Chosen-Ciphertext Security in Factoring-Based Encryption”, Advances in Cryptology – Asiacrypt 2006.

## Idea of Security for RSA-OAEP

$$\mathcal{E}_{pk}(m, r) = \text{RSA}(s = (m||0^{k_1}) \oplus G(r), t = r \oplus H(s)) \rightarrow c$$

Guess 1 bit of  $M = m||0^{k_1} \Leftrightarrow$  Guess  $r \Leftrightarrow$  Guess  $s \Leftrightarrow$  Guess  $(s, t)$   
 $\Leftrightarrow$  Inverse RSA

$$\mathcal{D}(c) = c^d \bmod n \rightarrow (s, t), r = H(s) \oplus t, \text{ and } m||0^{k_1} = s \oplus G(r)$$

Valid encryption  $\Leftrightarrow H(s)$  and  $G(r) \Leftrightarrow$  Plain-text

# Outline

- 1 Recall
- 2 Block cipher modes
  - ECB
  - CBC
  - CFB
  - OFB
- 3 Attack on ECB
- 4 Hybrid Encryption
- 5 OAEP
- 6 Logical Attacks**
- 7 Needham Schroeder
- 8 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

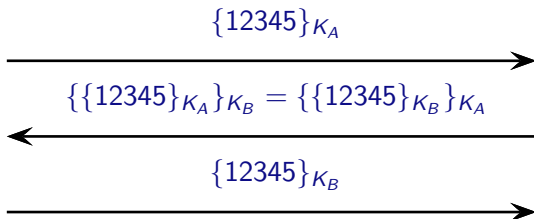
## Another Simple Example using RSA

 $\{12345\}_{K_A}$ 

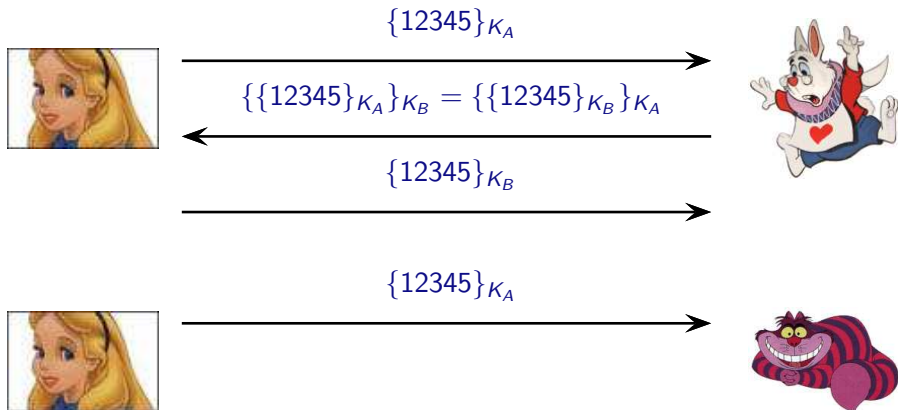
## Another Simple Example using RSA

 $\{12345\}_{K_A}$  $\{\{12345\}_{K_A}\}_{K_B} = \{\{12345\}_{K_B}\}_{K_A}$ 

## Another Simple Example using RSA

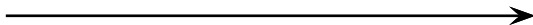


## Another Simple Example using RSA



## Another Simple Example using RSA



$$\{12345\}_{K_A}$$


$$\{\{12345\}_{K_A}\}_{K_B} = \{\{12345\}_{K_B}\}_{K_A}$$


$$\{12345\}_{K_B}$$


$$\{12345\}_{K_A}$$


$$\{\{12345\}_{K_A}\}_{K_I} = \{\{12345\}_{K_I}\}_{K_A}$$


## Another Simple Example using RSA



$$\{12345\}_{K_A}$$


$$\{\{12345\}_{K_A}\}_{K_B} = \{\{12345\}_{K_B}\}_{K_A}$$


$$\{12345\}_{K_B}$$


$$\{12345\}_{K_A}$$


$$\{\{12345\}_{K_A}\}_{K_I} = \{\{12345\}_{K_I}\}_{K_A}$$

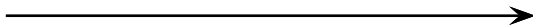

$$\{12345\}_{K_I}$$


## Another Simple Example using RSA

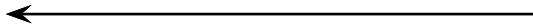


$$\{12345\}_{K_A}$$


$$\{\{12345\}_{K_A}\}_{K_B} = \{\{12345\}_{K_B}\}_{K_A}$$


$$\{12345\}_{K_B}$$


$$\{12345\}_{K_A}$$


$$\{\{12345\}_{K_A}\}_{K_I} = \{\{12345\}_{K_I}\}_{K_A}$$


$$\{12345\}_{K_I}$$


Problem of Authentication

## Examples of kinds of attack

- **Man-in-the-middle (or parallel sessions) attack:** pass messages through to another session  $A \leftrightarrow I \leftrightarrow B$ .
- **Replay (or freshness) attack:** record and later re-introduce a message or part.
- **Reflection attack:** send transmitted information back to originator.
- **Oracle attack:** take advantage of normal protocol responses as encryption and decryption “services”.
- **Type flaw (confusion) attack:** substitute a different type of message field (e.g. a key vs. a name).

# Outline

- 1 Recall
- 2 Block cipher modes
  - ECB
  - CBC
  - CFB
  - OFB
- 3 Attack on ECB
- 4 Hybrid Encryption
- 5 OAEP
- 6 Logical Attacks
- 7 Needham Schroeder**
- 8 Conclusion

## Messages Abstraction

- Names:  $A$ ,  $B$  or Alice, Bob, ...
- Nonces:  $N_A$ . Fresh data.
- Keys:  $K$  and **inverse keys**  $K^{-1}$
- Asymmetric Encryption:  $\{M\}_{K_A}$
- Symmetric Encryption:  $\{M\}_{K_{AB}}$ .
- Message concatenation:  $\langle M_1, M_2 \rangle$ .

Example:  $\{\langle A \oplus N_B, K_{AB} \rangle\}_{K_B}$ .

## Example: Needham-Schroeder Protocol 1978



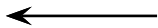
$\{N_A, A\}_{K_B}$



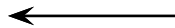
## Example: Needham-Schroeder Protocol 1978



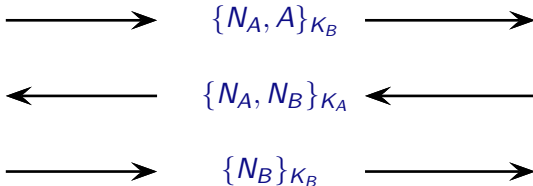
$\{N_A, A\}_{K_B}$



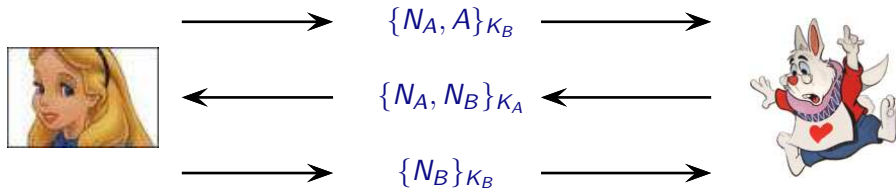
$\{N_A, N_B\}_{K_A}$



## Example: Needham-Schroeder Protocol 1978



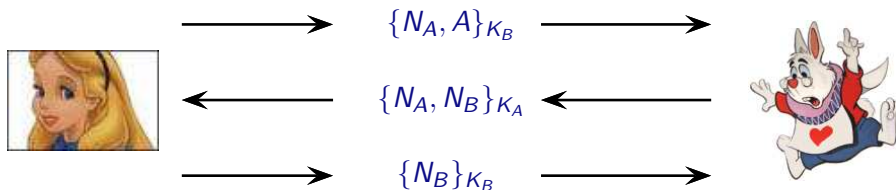
## Example: Needham-Schroeder Protocol 1978



### 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!

## Exercise

### Answer

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

Exercise: Try to Find for the next lecture this famous attack.

# Questions?

## How can we find such attacks?

- Models for Protocols
- Models for Properties
- Theories
- Dedicated Techniques
- Tools
  - Automatic
  - Semi-automatic

## Why is it difficult to verify such protocols?

- Messages: Size not bounded
- Nonces: Arbitrary number
- Channel: Unsecure
- Intruder: Unlimited capabilities
- Instances: Unbounded numbers of principals
- Interleaving: Unlimited applications of the protocol.

## What about Computational Security for Needham Schroeder ?

“A Computational Analysis of the Needham Schroeder Lowe Protocol” by Bogdan Warinschi in Journal of Computer Security; 13(3), pp: 565–591, 2005.

If encryption scheme is IND-CCA then Needham Schroeder Lowe Protocol is indeed a secure mutual authentication protocol.

## Link between Computational and Symbolic

“Reconciling Two Views of Cryptography (The Computational Soundness of Formal Encryption)” 2000, by Martin Abadi, Phillip Rogaway in IFIP International Conference on Theoretical Computer Science.

Using an hybrid Argument ;-)

# Outline

- 1 Recall
- 2 Block cipher modes
  - ECB
  - CBC
  - CFB
  - OFB
- 3 Attack on ECB
- 4 Hybrid Encryption
- 5 OAEP
- 6 Logical Attacks
- 7 Needham Schroeder
- 8 Conclusion**

# Summary

## Today

- ECB, CBC, FBC, OFB
- Attack on ECB
- Hybrid Encryption
- OAEP
- Logical Attacks
- Needham Schroeder

## Where are we?

- Introduction
- Indistinguishability
- Public Encryption
- Symmetric encryption ★
- Security protocols:
  - Symbolic Model
  - Computational Model
- Non-interference Problem
- Access Control and Security Policies
- And a little more, if possible...

## Next Time

- Symbolic Model: Principles using Examples
- Playing with Tools:
  - Scyther
  - Avispa: OFMC, CI-Atse, SATMC, TA4SP
  - Proverif

**Thank you for your attention.**

**Questions ?**