

# Models and analysis of security protocols

## 1st Semester 2009-2010

### Security Protocols

### Lecture 6

**Pascal Lafourcade**

*Université Joseph Fourier, Verimag*

Master: October 05th 2009

## Last Time (I)

### Symmetric encryption and Protocols

- ▶ ECB, CBC, FBC, OFB
- ▶ Attack on ECB
- ▶ Hybrid Encryption
- ▶ OAEP

Remarks, questions, comments ?

## Last Time (II)

### Exercises done

- ▶ CBC Attacks

## Outline of Today:

Logical Attacks

Diffie-Hellman

Needham Schroeder

Dolev Yao's Intruder

Undecidability for unbounded number of sessions

Conclusion

# Outline

## Logical Attacks

Diffie-Hellman

Needham Schroeder

Dolev Yao's Intruder

Undecidability for unbounded number of sessions

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



Day After



## Simple Example



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



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



Day After



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



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



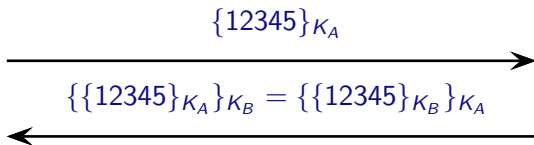
This kind of attack is valid for all encryptions

## Another Simple Example using RSA

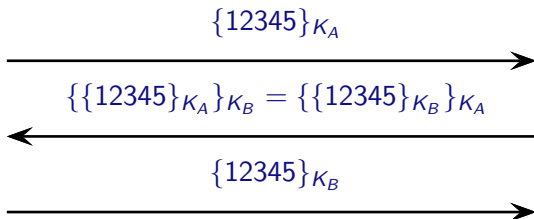
$\{12345\}_{K_A}$



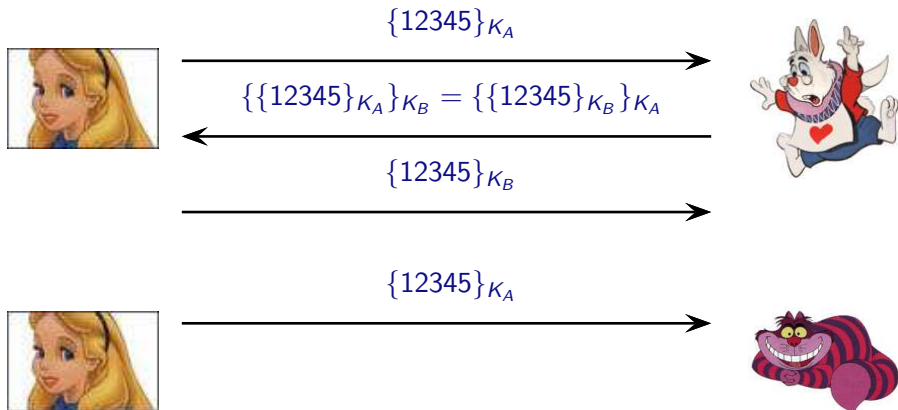
## Another Simple Example using RSA



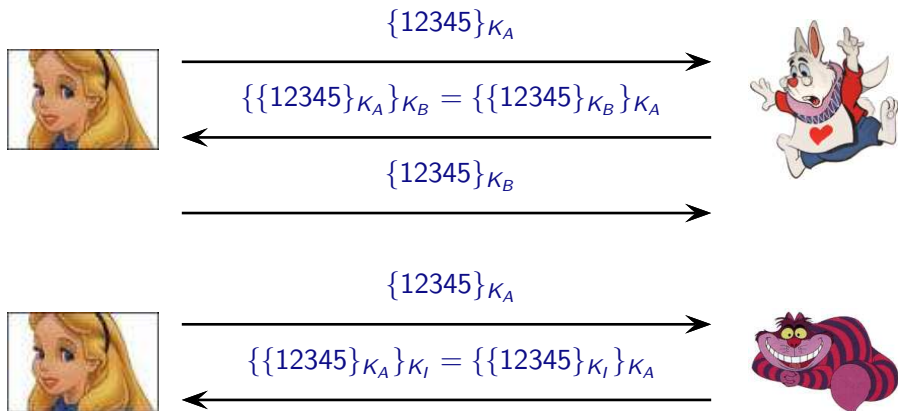
## Another Simple Example using RSA



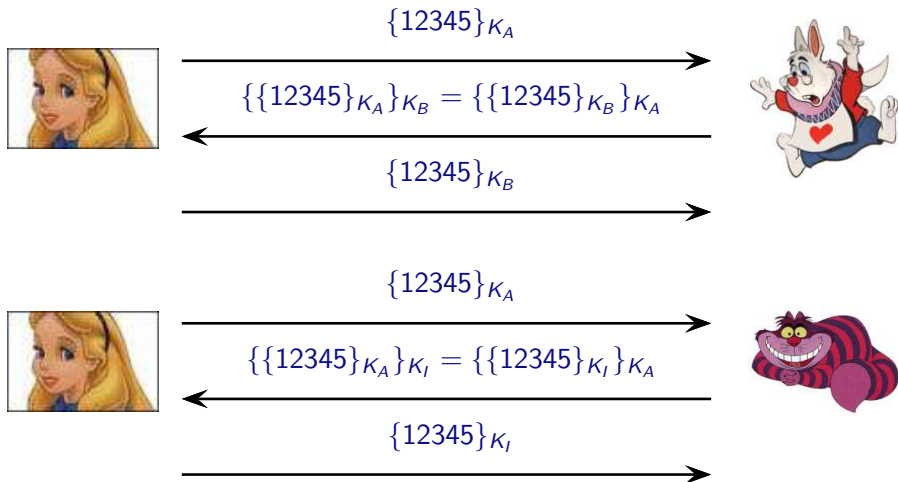
## Another Simple Example using RSA



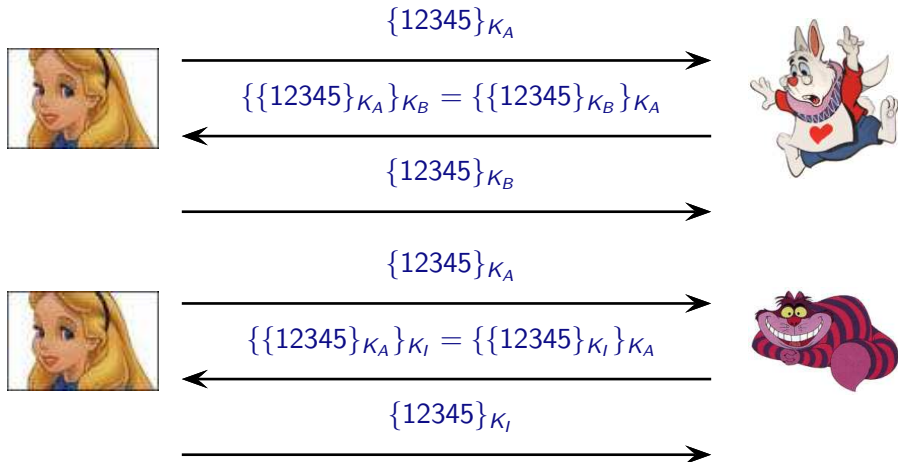
## Another Simple Example using RSA



## Another Simple Example using RSA



## Another Simple Example using RSA



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

Logical Attacks

**Diffie-Hellman**

Needham Schroeder

Dolev Yao's Intruder

Undecidability for unbounded number of sessions

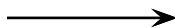
Conclusion

# The Diffie-Hellman protocol

$g, p$  are public parameters.



$$g^x \bmod p$$



Diffie chooses  $x$  and computes  $g^x \bmod p$ .

Hellman chooses  $y$  and computes  $g^y \bmod p$ .

**Basic Diffie-Hellman key-exchange:** initiator I and responder R exchange public “half-keys” to arrive at mutual session key  $k = g^{xy} \bmod p$ .

## The Diffie-Hellman protocol

$g, p$  are public parameters.



$$g^x \bmod p$$



$$g^y \bmod p$$

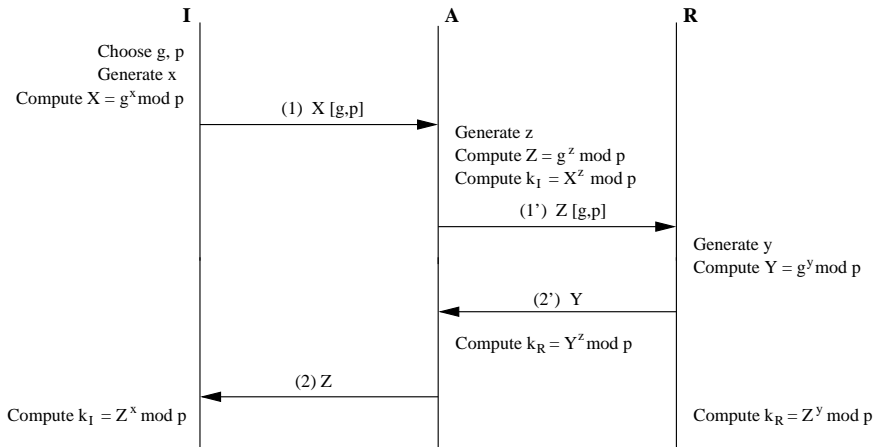


Diffie chooses  $x$  and computes  $g^x \bmod p$ .

Hellman chooses  $y$  and computes  $g^y \bmod p$ .

**Basic Diffie-Hellman key-exchange:** initiator I and responder R exchange public “half-keys” to arrive at mutual session key  $k = g^{xy} \bmod p$ .

# Man-in-the-middle attack



# Outline

Logical Attacks

Diffie-Hellman

**Needham Schroeder**

Dolev Yao's Intruder

Undecidability for unbounded number of sessions

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

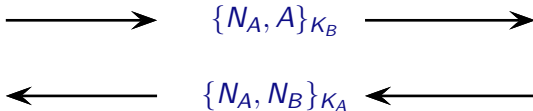
## Example: Needham-Schroeder Protocol 1978



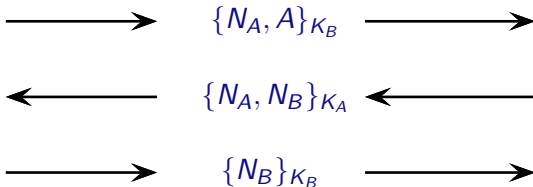
$\{N_A, A\}_{K_B}$



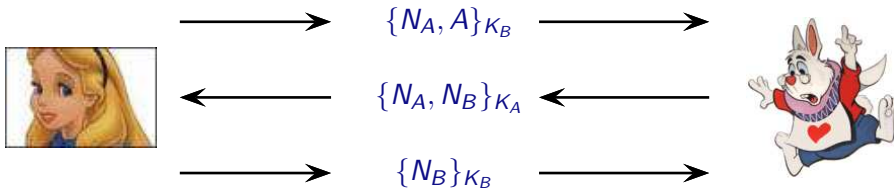
## Example: Needham-Schroeder Protocol 1978



## Example: Needham-Schroeder Protocol 1978



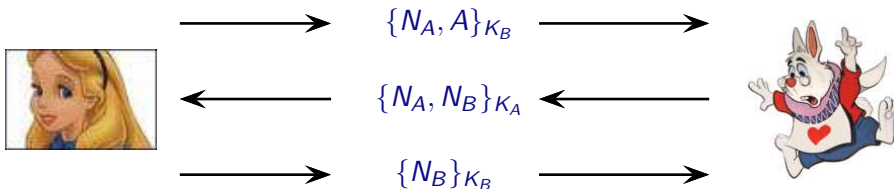
## Example: Needham-Schroeder Protocol 1978



### 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!

# Low Attack on the Needham-Schroeder

so-called “Man in the middle attack”



Agent A



Intruder I



Agent B

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

# Lowé Attack on the Needham-Schroeder

so-called “Man in the middle attack”



Agent A

$\{A, N_a\}_{K_I}$  →



Intruder I

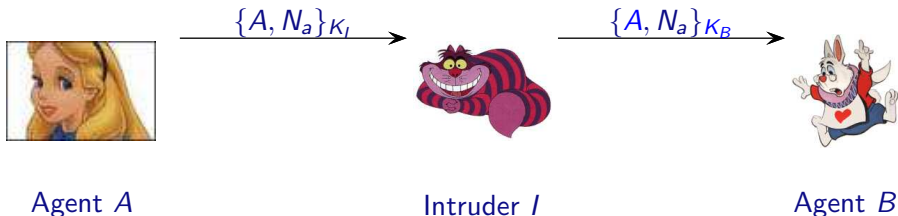


Agent B

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

# Lowé Attack on the Needham-Schroeder

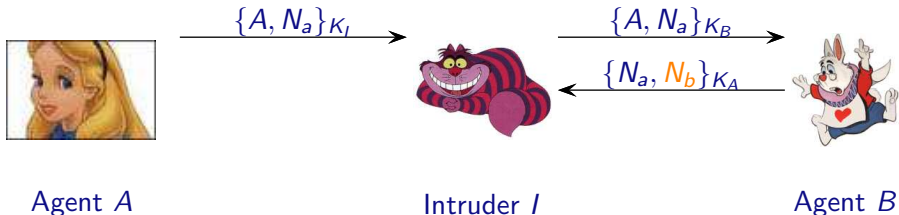
so-called “Man in the middle attack”



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

# Lowé Attack on the Needham-Schroeder

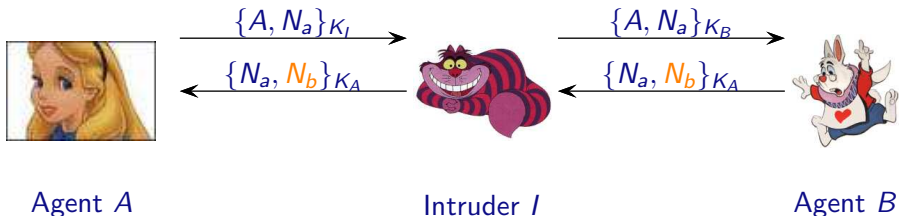
so-called “Man in the middle attack”



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

# Lowé Attack on the Needham-Schroeder

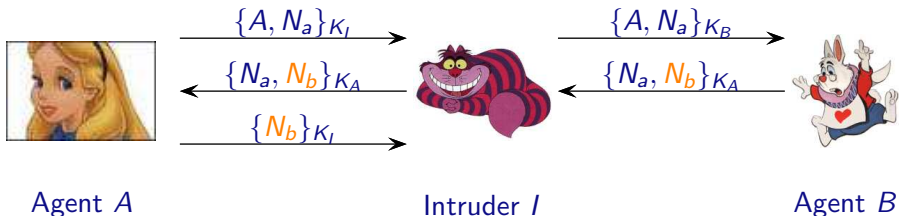
so-called “Man in the middle attack”



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

# Lowé Attack on the Needham-Schroeder

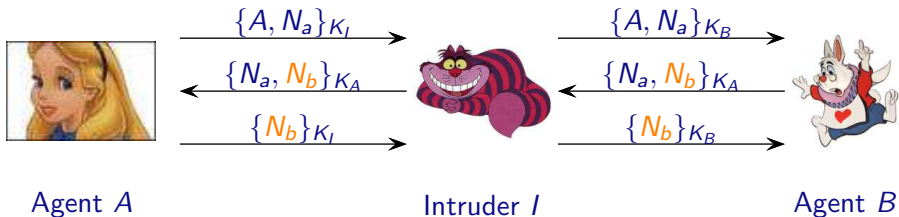
so-called “Man in the middle attack”



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

# Lowé Attack on the Needham-Schroeder

so-called “Man in the middle attack”



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

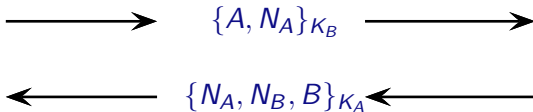
## Needham-Schroeder corrected by Lowe 1995



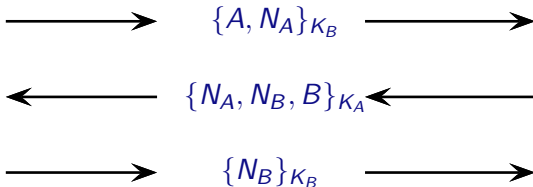
$\{A, N_A\}_{K_B}$



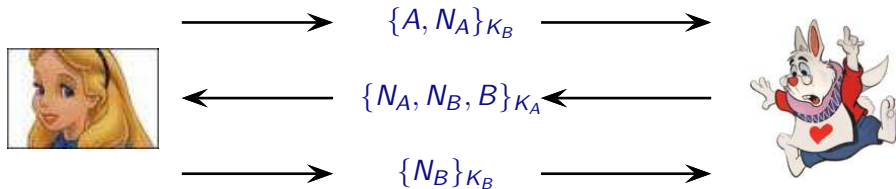
## Needham-Schroeder corrected by Lowe 1995



## Needham-Schroeder corrected by Lowe 1995



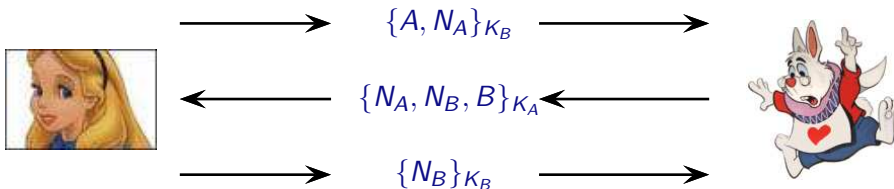
## Needham-Schroeder corrected by Lowe 1995



### Question

- This time the protocol is secure?

## Needham-Schroeder corrected by Lowe 1995



### Question

- ▶ This time the protocol is secure?

### Answer

- ▶ There exists a type flaw attack.

## Type flaw attacks

- ▶ A message consists of a sequence of sub-messages.  
Examples: a principal's name, a nonce, a key, ...

- ▶ Messages sent as bit strings. No type information.

1011 0110 0010 1110 0011 0111 1010 0000

- ▶ **Type flaw** is when  $A \rightarrow B : M$  and  $B$  accepts  $M$  as valid but parses it differently. I.e.,  $B$  interprets the bits differently than  $A$ .
- ▶ **Example:** two 16-bit nonces  $\{N_A, N_B\}$  could be mistaken as a 32-bit shared key.  
Let's consider several examples from actual protocols.

## Type Flaw Attack on the Needham-Schroeder-Lowe



Agent A



Intruder I



Agent B

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

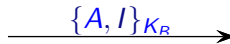
## Type Flaw Attack on the Needham-Schroeder-Lowe



Agent A



Intruder I



Agent B

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

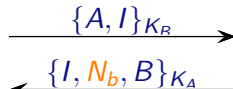
## Type Flaw Attack on the Needham-Schroeder-Lowe



Agent A



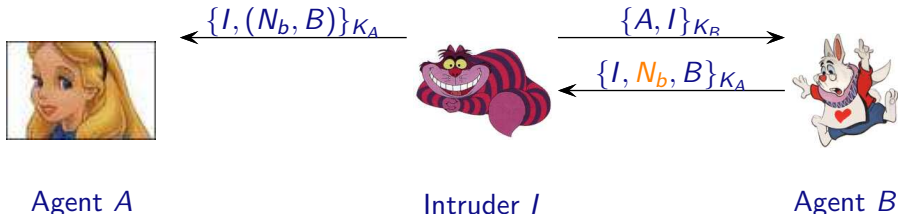
Intruder I



Agent B

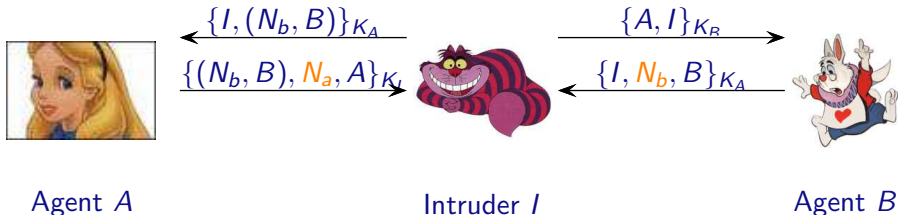
- $A \longrightarrow B : \{A, N_a\}_{K_B}$
- $B \longrightarrow A : \{N_a, N_b, B\}_{K_A}$
- $A \longrightarrow B : \{N_b\}_{K_B}$

## Type Flaw Attack on the Needham-Schroeder-Lowe



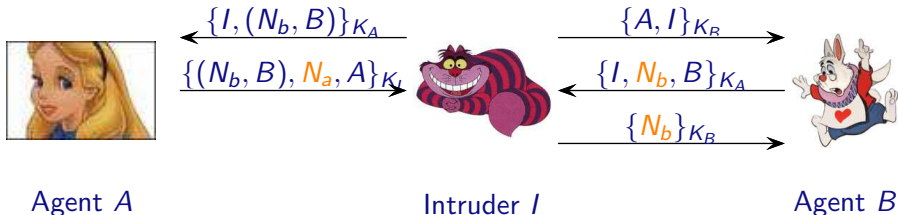
- $A \longrightarrow B : \{A, N_a\}_{K_B}$   
 $B \longrightarrow A : \{N_a, N_b, B\}_{K_A}$   
 $A \longrightarrow B : \{N_b\}_{K_B}$

## Type Flaw Attack on the Needham-Schroeder-Lowe



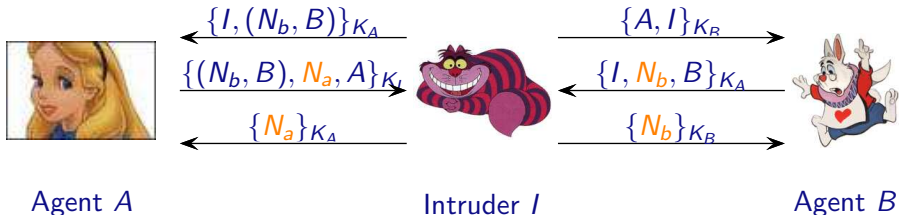
- $A \longrightarrow B : \{A, N_a\}_{K_B}$
- $B \longrightarrow A : \{N_a, N_b, B\}_{K_A}$
- $A \longrightarrow B : \{N_b\}_{K_B}$

# Type Flaw Attack on the Needham-Schroeder-Lowe



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

## Type Flaw Attack on the Needham-Schroeder-Lowe



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

## Another Type Flaw Attack: Otway-Rees Protocol

### Otway-Rees

- 1  $A \rightarrow B : (M, A, B, (N_A, M, A, B)_{K_{as}})$
- 2  $B \rightarrow S : (M, A, B, (N_A, M, A, B)_{K_{as}}, (N_B, M, A, B)_{K_{bs}})$
- 3  $S \rightarrow B : (M, (N_A, K_{ab})_{K_{as}}, (N_B, K_{ab})_{K_{bs}})$
- 4  $B \rightarrow A : (M, (N_A, K_{ab})_{K_{as}})$

where  $M$  is the session-identifier.

## Another Type Flaw Attack: Otway-Rees Protocol

### Otway-Rees

- 1  $A \rightarrow B : (M, A, B, (N_A, M, A, B)_{K_{as}})$
- 2  $B \rightarrow S : (M, A, B, (N_A, M, A, B)_{K_{as}}, (N_B, M, A, B)_{K_{bs}})$
- 3  $S \rightarrow B : (M, (N_A, K_{ab})_{K_{as}}, (N_B, K_{ab})_{K_{bs}})$
- 4  $B \rightarrow A : (M, (N_A, K_{ab})_{K_{as}})$

where  $M$  is the session-identifier.

### Attack

- 1  $A \rightarrow B : (M, A, B, (N_A, M, A, B)_{K_{as}})$
- 2  $B \rightarrow I(S) : (M, A, B, (N_A, M, A, B)_{K_{as}}, (N_B, M, A, B)_{K_{bs}})$
- 3  $I(S) \rightarrow B : (M, (N_A, M, A, B)_{K_{as}}, (N_B, M, A, B)_{K_{bs}})$
- 4  $B \rightarrow A : (M, (N_A, M, A, B)_{K_{as}})$

## 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 ;-)

# 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: Insecure
- ▶ Intruder: Unlimited capabilities
- ▶ Instances: Unbounded numbers of principals
- ▶ Interleaving: Unlimited applications of the protocol.

# Outline

Logical Attacks

Diffie-Hellman

Needham Schroeder

**Dolev Yao's Intruder**

Undecidability for unbounded number of sessions

Conclusion

## The Intruder is the Network (Worst Case)



## The Intruder is the Network (Worst Case)



Listen

Passive: Intruder deduction problem

## The Intruder is the Network (Worst Case)



Listen

Intercept message

(Re)play message

Delete message

Passive: Intruder deduction problem

Active: Security problem

## The Intruder is the Network (Worst Case)



Listen

Intercept message

(Re)play message

Delete message

Passive: Intruder deduction problem

Active: Security problem

### Intruder Capabilities (Dolev-Yao Model 80's)

- ▶ Encryption, Decryption with a key
- ▶ Pairing, Projection.

# Dolev-Yao 1982

- ▶ Intruder controls the network and can:
  - ▶ intercept messages
  - ▶ modify messages
  - ▶ block messages
  - ▶ generate new messages
  - ▶ insert new messages
- ▶ Perfect cryptography:
  - ▶ Abstraction with terms algebra
  - ▶ Decryption only if inverse key is known
- ▶ Protocol has
  - ▶ Arbitrary number of principals
  - ▶ Arbitrary number of parallel sessions
  - ▶ Messages with arbitrary size

## Proof System

A **sequent** is an expression of the form  $T \vdash u$ .

### Definition

A **proof** of a sequent  $T \vdash u$  is a tree whose nodes are labeled by either sequents or expressions of the form " $v \in T$ ", such that:

- ▶ Each leaf is labeled by an expression of the form  $v \in T$ , and each non-leaf node is labeled by an sequent.
- ▶ Each node labeled by a sequent  $T \vdash v$  has  $n$  children labeled by  $T \vdash s_1, \dots, T \vdash s_n$  such that there is an instance of an inference rule with conclusion  $T \vdash_E v$  and **hypotheses**  $T \vdash s_1, \dots, T \vdash s_n$ .
- ▶ The **root** of the tree is labeled by  $T \vdash u$ .

A **subproof** of a proof  $P$  is a subtree of  $P$ .

## Notions for Proof System

### Definition

- ▶ **Size of a proof**  $P$  of  $T \vdash u$  is denoted by  $|P|$ , is the number of nodes in the proof.
- ▶ A proof  $P$  of  $T \vdash u$  is **minimal** if there does not exist a proof  $P'$  of  $T \vdash u$  such that  $|P'| < |P|$ .

## Dolev-Yao Deduction System

Deduction System :  $T_0 \vdash^? s$

$$(A) \quad \frac{u \in T_0}{T_0 \vdash u}$$

$$(UL) \quad \frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash u}$$

$$(P) \quad \frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash \langle u, v \rangle}$$

$$(UR) \quad \frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash v}$$

$$(C) \quad \frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash \{u\}_v}$$

$$(D) \quad \frac{T_0 \vdash \{u\}_v \quad T_0 \vdash v}{T_0 \vdash u}$$

Example:  $T_0 \vdash? s$

### Example

$T_0 = \{k, \{b\}_c, \langle a, \{c\}_k \rangle\}$  and  $s = b$

Example:  $T_0 \vdash^? s$

### Example

$T_0 = \{k, \{b\}_c, \langle a, \{c\}_k \rangle\}$  and  $s = b$

$$\begin{array}{c}
 \begin{array}{c}
 (A) \frac{\langle a, \{c\}_k \rangle \in T_0}{T_0 \vdash \langle a, \{c\}_k \rangle} \\
 (UR) \frac{}{T_0 \vdash \{c\}_k} \\
 (A) \frac{k \in T_0}{T_0 \vdash k}
 \end{array} \\
 \hline
 \begin{array}{c}
 (A) \frac{\{b\}_c \in T_0}{T_0 \vdash \{b\}_c} \\
 (D) \frac{}{T_0 \vdash c}
 \end{array} \\
 \hline
 (D) \frac{}{T_0 \vdash b}
 \end{array}$$

Exercise:  $T_0 \vdash? s$

Is it possible from  $T_0$  to deduce  $s$

- ▶  $T_0 = \{a, k\}$  and  $s = \langle a, \{a\}_k \rangle$
- ▶  $T_0 = \{a, k\}$  and  $s = \langle b, \{k\}_a \rangle$
- ▶  $T_0 = \{\{k\}_a, b\}$  and  $s = \langle \{b\}_{\{k\}_a}, \{k\}_a \rangle$
- ▶  $T_0 = \{\langle a, \{k\}_a \rangle\}$  and  $s = \{\langle a, \{k\}_a \rangle\}_k$

# Outline

Logical Attacks

Diffie-Hellman

Needham Schroeder

Dolev Yao's Intruder

Undecidability for unbounded number of sessions

Conclusion

## Main Results

In general security problem **undecidable** [DLMS'99, AC'01]

Bounded number of session  $\Rightarrow$  **Decidability** [AL'00, RT'01]

# Undecidability

## Definition (Post Correspondence Problem (PCP))

Let  $\Sigma$  be a finite alphabet.

**Input** : Sequence of pairs  $\langle u_i, v_i \rangle_{1 \leq i \leq n}$   $u_i, v_i \in \Sigma^*$ ,  $n \in \mathbb{N}$

**Question** : Existence of  $k, i_1, \dots, i_k \in \mathbb{N}$  such that

$$u_{i_1} \dots u_{i_k} = v_{i_1} \dots v_{i_k}?$$

# Undecidability

## Definition (Post Correspondence Problem (PCP))

Let  $\Sigma$  be a finite alphabet.

**Input** : Sequence of pairs  $\langle u_i, v_i \rangle_{1 \leq i \leq n}$   $u_i, v_i \in \Sigma^*$ ,  $n \in \mathbb{N}$

**Question** : Existence of  $k, i_1, \dots, i_k \in \mathbb{N}$  such that

$$u_{i_1} \dots u_{i_k} = v_{i_1} \dots v_{i_k}?$$

## Example

$u_1$	$u_2$	$u_3$	$u_4$	$v_1$	$v_2$	$v_3$	$v_4$
<i>aba</i>	<i>bbb</i>	<i>aab</i>	<i>bb</i>	<i>a</i>	<i>aaa</i>	<i>abab</i>	<i>babba</i>

Solution: **1431**

$$u_1 \cdot u_4 \cdot u_3 \cdot u_1 = aba \cdot bb \cdot aab \cdot aba = a \cdot babba \cdot abab \cdot a = v_1 \cdot v_4 \cdot v_3 \cdot v_1$$

But no solution for  $\langle \mathbf{u}_1, \mathbf{v}_1 \rangle, \langle \mathbf{u}_2, \mathbf{v}_2 \rangle, \langle \mathbf{u}_3, \mathbf{v}_3 \rangle$

# Undecidability

## Definition (Post Correspondence Problem (PCP))

Let  $\Sigma$  be a finite alphabet.

**Input** : Sequence of pairs  $\langle u_i, v_i \rangle_{1 \leq i \leq n}$   $u_i, v_i \in \Sigma^*$ ,  $n \in \mathbb{N}$

**Question** : Existence of  $k, i_1, \dots, i_k \in \mathbb{N}$  such that

$$u_{i_1} \dots u_{i_k} = v_{i_1} \dots v_{i_k}?$$

## Example

$u_1$	$u_2$	$u_3$	$u_4$	$v_1$	$v_2$	$v_3$	$v_4$
<i>aba</i>	<i>bbb</i>	<i>aab</i>	<i>bb</i>	<i>a</i>	<i>aaa</i>	<i>abab</i>	<i>babba</i>

Solution: **1431**

$$u_1 \cdot u_4 \cdot u_3 \cdot u_1 = aba \cdot bb \cdot aab \cdot aba = a \cdot babba \cdot abab \cdot a = v_1 \cdot v_4 \cdot v_3 \cdot v_1$$

But no solution for  $\langle \mathbf{u}_1, \mathbf{v}_1 \rangle, \langle \mathbf{u}_2, \mathbf{v}_2 \rangle, \langle \mathbf{u}_3, \mathbf{v}_3 \rangle$

PCP is undecidable

## Undecidability for Protocols

We construct a protocol such that decidability of secret implies decidability of PCP.

$$A : \text{send}(\{\langle u_i, v_i \rangle\}_{K_{ab}}) \quad (1 \leq i \leq n)$$

$$B : \text{receive}(\{\langle x, y \rangle\}_{K_{ab}}) \\ \text{send}(\{\langle \langle x \cdot u_i, y \cdot v_i \rangle \rangle_{K_{ab}}, \{s\}_{\langle \langle x \cdot u_i, x \cdot u_i \rangle \rangle_{K_{ab}}}\}) \quad (1 \leq i \leq n)$$

We assume that  $\mathbf{K}_{AB}$  is a shared key between **A** and **B**.

Intruder can find  $\mathbf{s}$  iff he can solve PCP.

# Outline

Logical Attacks

Diffie-Hellman

Needham Schroeder

Dolev Yao's Intruder

Undecidability for unbounded number of sessions

Conclusion

# Summary

## Today

- ▶ Diffie Hellman
- ▶ Needham Schroeder
- ▶ Dolev Yao Intruder
- ▶ Undecidability Result

# Next Time

## Passive Intruder

- ▶ Locality

**Thank you for your attention.**

**Questions ?**