

Models and Analysis for Security Protocols

1st Semester 2007/2008

P. Lafourcade.

SET 1

Date: 11.10.2007

Exercise 1

Give the security properties that an international airport should guarantee.

Exercise 2

1. $A \rightarrow B : \{N_a, A\}_{pk(B)}$
2. $A \leftarrow B : \{N_a, N_b\}_{pk(A)}$
3. $A \rightarrow B : \{N_b\}_{pk(B)}$

- Try to Find an attack on Needham-Schroeder protocol.
- Try to correct the potocol to avoid this attack.
- Try to find a flaw on the protocol corrected by Gavin Lowe.

Exercise 3

Symmetric Cryptosystems Decrypt the following ciphers (they all correspond to an encryption method seen in class):

1. (very easy) 20-8-5-13-15-19-20-9-13-16-15-18-20-1-14-20-20-8-9-14-7-9-14-3-15-13-13-21-14-9-3-1-20-9-15-14-9-19-20-15-8-5-1-18-23-8-1-20-9-19-14-20-2-5-9-14-7-19-1-9-4
2. (easy) FDWV DUH LQWHQGHG WR WHOO XV WKDW QRW HYHUBWKLQJ LQ QDWXUH KDV D IXQFWLRQ.
(Hint: B.C.)
3. (medium) OUFWIY ATNHAT DONNIG GHRTEI TYOODI ELRFUS
(Hint: observe the structure of the ciphertext)
4. (hard) JF CFEX REU KYREBJ WFI RCC KYV WZJY
(Hint: ROT-N)
5. (hard)
ESIRNDVYIUPEOGCRDFNAOIYOTGSORIRCUAOEORNNSVOCISEWE
(Hint: The cipher has 50 letters)

Exercise 4

Funny Cryptosystem



- **History:**

- This ciphertext appeared engraved on a tombstone in Trinity Churchyard (New York) in 1794.
- First published solution: 1896.

- **Questions:**

1. What kind of cipher is it?
2. Why is it so difficult to break? (Especially without the hint!)
3. What is the plaintext message?
4. What is the key?

- HINT: TIC TAC TOE =

Exercise 5

Find the unifier of the following terms t and u

1. $t = a \quad u = X$
2. $t = p(a, X) \quad u = p(Y, b)$
3. $t = p(f(X), g(Z)) \quad u = p(f(a), Y)$

Exercise 6

Prove McAllester theorem.

If a proof system P is SyntacticSubterm-local then there is a P-time procedure to decide the deductibility in P .