SECURITY IN NETWORKED COMPUTING SYSTEMS

Master in Computer Engineering, Master in Embedded Computing Systems

16 February 2016

Candidate ______________________________________ **Serial no.** _________________

EXERCISE NO. 1 — #MARKS: 12

(1) Describe the Diffie-Hellmann protocol
(2) Argue about its security w.r.t. a passive adversary
(3) Argue about its security w.r.t. a MITM attack

EXERCISE NO. 2 — #MARKS: 12

Alice and Bob use one-time pad (OTP) and have agreed on a perfectly random key K. Alice will send Bob the answer to the question "Are you taking SNCS?" as either 'Y' or 'N' encoded in their ASCII representation (1011001 and 1001110, respectively). The adversary knows nothing about the key but intercepts the cipher-text c exchanged between Alice and Bob: 1001110.

(1) What cipher-text c' should the adversary send Bob to flip Alice's message?
(2) Alice decides to use a secure hash function $h(\cdot)$ and transmits the cypher-text c'' obtained from enciphering $m||\mathrm{h}(m)$, where m is the clear-text message and || is the concatenation operator. Can it be of any help?
(3) Without using anything other than OTP, how can Alice and Bob solve this problem? (Hint: use two keys)

EXERCISE NO. 3 — #MARKS: 6

1. What are certificates for?
   A. Establishing an indissoluble link between an identifier and a public key.
   B. Establishing an indissoluble link between a public key and the owner of the certificate.
   C. Establishing the privileges of the owner of the certificate.
   D. Establishing the trustworthiness of the certificate owner.
2. What are the Certification Authority's obligations before releasing a certificate?
3. Describe the minimum set of data fields that you expect to find in a certificate.

SECURITY IN NETWORKED COMPUTING SYSTEMS

Master in Computer Engineering, Master in Embedded Computing Systems

16 February 2016

SOLUTION

EXERCISE N.1

See theory.

EXERCISE N.2

Question 1.

Let c = msg □ K where msg may assume two values mY and mN. In order to flip Alice's message, the adversary has to transmit c' = $c \oplus (mY \oplus mN)$.

Substituting the exercise data we obtain the following. $(mY \oplus mN)$ = 1011001 ⊕ 1001110 = 0010111. Therefore, c' = $c \oplus (mY \oplus mN)$ = 1001110 ⊕ 0010111 = 1011001.

Question 2.

No. Let c = $(msg||H(msg) \oplus K$ where msg may assume two values mY and mN. In order to flip Alice's message, the adversary has to transmit the cipher-text c' s.t.

$$c' = c \oplus (mY||\mathrm{H}(mY) \oplus (mN||\mathrm{H}(mN)).$$

Question 3.

A possible solution requires two keys, KN and KY such that $KY \oplus KN \neq mY \oplus mN$ (*Uniqueness condition*). Alice and Bob share these keys. Alice transmits c such that

$$c = \begin{cases} mY \oplus \mathrm{KY} & if\ answer\ is\ yes \\ mN \otimes \mathrm{KN} & if\ answer\ is\ no \end{cases}$$

Upon receiving a cipher text c, Bob i) computes $\overline{mY} = c \oplus \mathrm{kY}$, $\overline{mN} = c \oplus \mathrm{KN}$; and, ii) returns message m such that:

$$m = \begin{cases} mY & if\ \bar{m}Y = mY \\ mN & f\ \bar{m}N = mN \\ \perp & otherwise \end{cases}$$

The Uniqueness Condition guarantees that mN cannot be derived from cY and vice versa. Notice that in order to flip Alice's answer the adversary must be able to obtain cN from cY and vice versa. This requires the adversary to know $KY \oplus KN$. However, this is not possible given the Uniqueness condition, the secrecy and randomness of the keys.

SECURITY IN NETWORKED COMPUTING SYSTEMS

Master in Computer Engineering, Master in Embedded Computing Systems

16 February 2016

EXERCISE N.3

Question 1. Option B.

Question 2. Identify the subject and authenticate the key.

Question 3. Subject identifier (S), public key (pK), validity period (V), a digital signature on S||pK||V by the Certification Authority.