SICUREZZA NELLE RETI   SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)

Laurea Specialistica in Ingegneria Informatica   ***Laurea Magistrale in Ingegneria Informatica***

SECURITY IN NETWORKED COMPUTING SYSTEMS

Computer Engineering

15 June 2015

EXERCISE NO. 1   #MARKS: 10

With reference to the Diffie-Hellmann key establishment scheme,

1. Describe the scheme;
2. Argue its security with respect to a passive adversary;
3. Argue its security with respect to an active adversary.

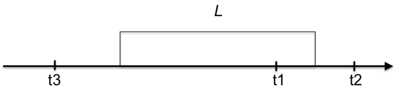
EXERCISE NO. 2   #MARKS: 10

Let us consider an implementation of One-Time Pad (OTP) on *n* bit that makes it a perfect cipher.

1. Let $k_0 = \overbrace{000\ldots000}^{n}$ be a key and m an *n*-bit message. Compute the cipher-text $c = m \oplus k_0$.
2. Is there any advantage, or disadvantage, in removing key k_0 from the set of possible keys?
3. Let us suppose that c = `"The password of my bank account is my wife's birthday"`. Which are the most probable plaintext messages (determine at least two)? Which are the corresponding keys?

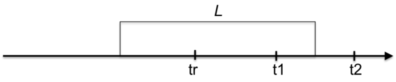
EXERCISE NO. 3   #marks: 10

Let us consider the “simplified” certificate $Cert_A = A, pubK_A, L, \sigma$, with $\sigma = S_{CA}(t)$ and $t = H(A, || pubK_A || L)$, where *A* is the user identifier, $pubK_A$ is the user’s public key, *L* is the validity period, *H* is a collision-resistant hash function and *S* is a secure digital signature scheme.



With reference to the figure on the right, give a motivated answer to the following questions:

1. Is $Cert_A$ valid at time *t* = t1?
2. Is $Cert_A$ valid at time *t* = t2?
3. Is $Cert_A$ valid at time *t* = t3?



With reference to the figure on the right, assume that $Cert_A$ has been revoked at time *t* = tr, give a motivated answer to the following questions:

4. Is $Cert_A$ certainly present in CRL at time *t* = t1?
5. Is $Cert_A$ certainly present in CRL at time *t* = t2?

SICUREZZA NELLE RETI   SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)

Laurea Specialistica in Ingegneria Informatica   *Laurea Magistrale in Ingegneria Informatica*

SECURITY IN NETWORKED COMPUTING SYSTEMS

Computer Engineering

15 June 2015

SOLUTION

Exercise n.1

See theory.

Exercise n.2

Question 1.

$c = m$

Question 2.

If you remove k_0, than the number of keys become $2^n - 1$. It follows that the number of keys becomes smaller than the number of messages and therefore the resulting cipher is not perfect anymore.

Question 3.

Four possible messages are:

```
The password of my bank account is my wife's birthday
The password of my bank account is my aunt's birthday
The password of my bank account is b4nk-P4ssw0rd12345
Love of my life you left me. You have broken my heart
```

The respective keys are obtained by computing $k_i = c \oplus m_i$.

Exercise n. 3

1: valid
2, 3: invalid as outside the validity interval

4: the certificate is certainly in CRL

5: the certificate may not be in CRL because, it is not valid anymore, it might have been removed to shorten the CRL itself.

SICUREZZA NELLE RETI SICUREZZA DEI SISTEMI SOFTWARE (6/9 CFU)

Laurea Specialistica in Ingegneria Informatica *Laurea Magistrale in Ingegneria Informatica*

SECURITY IN NETWORKED COMPUTING SYSTEMS

Computer Engineering

15 june 2015