P.Lafourcade, G.Marcadet

Session 4

Exercise 1 (Example of Diffie-Hellman Key)
Alice and Bob agree on following parameters: $p = 541$ and $g = 2$. Alice generates the secret number $a = 292$. On his side, Bob generates the number $b = 426$.

1. What is their secret key computed with the Diffie-Hellman key exchange protocol?
2. During the Diffie-Hellman key exchange protocol, Alice computes $A = g^a$ and sends it to Bob. In the same way, Bob computes $B = g^b$ and sends it to Alice. If Oscar sees A and B, explain why Oscar cannot easily deduce the secret key K shared between Alice and Bob?
3. Assume that Oscar is an active adversary, show how Oscar can decrypt all messages that Alice and Bob exchange.

Exercise 2 (Attack of the Needham-Schroeder Protocol)
Alice and Bob want to exchange a session key. Ivan shares the secret key A with Alice, and the secret key B with Bob. The Needham-Schroeder protocol is as follows:

i Alice sends $(\text{Alice}\|\text{Bob}\|\text{Random}_1)$ to Ivan.

ii Ivan creates a session key K and sends $E_A(\text{Random}_1\|\text{Bob}\|K\|E_B(K\|\text{Alice}))$ to Alice.

iii Alice sends $E_B(K\|\text{Alice})$ to Bob.

iv Bob sends $E_K(\text{Random}_2)$ to Alice.

v Alice sends $E_K(\text{Random}_2 - 1)$ to Bob.

1. To what is of use Random_1?
2. Why Alice resends the encryption $\text{Random}_2 - 1$?
3. If Eve is able to listen the exchanged messages and if she has a old session key, show how she can convince Bob that she is Alice.
4. What we can add to messages to avoid this problem? Why it is enough and what looks like this new protocol?

Exercise 3 (The key ring of a PGP certicate)
A certificate (or "key") PGP has several keys. This set of keys is sometimes called certificate key ring. Moreover, each key is composed of two parts: one public key, and one private key. The key ring always contains at least a *master key*, other keys are called subkeys. Moreover, all keys are sorted in signature keys and in encryption keys.

1. Is master key a signature key or an encryption key?
2. The validity of PGP certificate is based on signatures: which ones?
3. What to think of the lifespan of the master key?
4. It is always possible to add encryption subkeys to a PGP certificate. Is there an interest to possess several encryption subkeys?
5. What to think of the lifespan of encryption key?

6. It is always possible to add signature subkeys to a PGP certificate. Is there an interest to possess several signature subkeys? Explain why.

7. All subkey of a PGP certificate must be certified by the master key. Why?

Exercise 4 (Signature Based on the Idendity)
From 1984, Adi Shamir proposed a way to obtain signatures that are based on the identity. We describe this solution as follows, where H is a cryptographic hash function:

Key generation	i Choose two big prime numbers p and q, and compute $n = p \cdot q$. ii Choose e such that $\gcd(e, \varphi(n)) = 1$.
Public key	(n, e)
Private keys	Only known by the *Key Distributor Center*: (p, q). Generated by the KDC and only knows by the user of identity i: g_i such that $g_i^e = i \mod n$.
Signature	For a message m: • Pick randomly r; • Compute $t = r^e \mod n$; • Compute $s = g_i \cdot r^{H(t\|m)} \mod n$; • The signature of the message m is the pair (s, t).
Verification	Check if $s^e = i \cdot t^{H(t\|m)} \mod n$.

1. Show that the verification is correct.

2. How the KDC can generate g_i from i?

3. Why g_i must be keep secret?

4. On which hard problem this protocol is based?

Exercise 5 (Secure Shell)
On request of SSH connection by a client, the server replies by sending its public key K_p in plain text. The client saves in this memory (more specifically in the file `$HOME/.ssh/known_host`; if this key is already stored, the client compare it to the stored key and warn the user if there is any difference). The client select one session key k and sends it to the server in an encrypted way. The server decrypts the session key k. The client and the server can now communicate with the shared secret key k.

1. Why secure a session with symmetric encryption instead of asymmetric encryption?

2. Assuming that all messages in the above protocol are authenticated, explain why the next connections are confidential and authenticated.

3. If the first connection is not authenticated, how to explain that an active attacker can masquerade as a server.

4. Why the client must inform the user when the public key changed?

5. Why SSH is useful?