# Homework Assignment # 11

Due Date: Wednesday, December 6

1. We consider a system in which a key $K_{AB}$ is established using the Diffie-Hellman key exchange protocol, and the encryption keys $K^{(i)}$ are then derived by computing:

$$K^{(i)} = H(K_{AB} \parallel i) \tag{1}$$

where $i$ is just an integer, e.g., represented in a 16 bit field. These derived keys are used for the actual data encryption with a symmetric (private-key) algorithm. New keys are derived periodically during the communication session. Note that most hash function are very fast.

   (a) Assume DES is being used as the data encryption algorithm. Which attack can be prevented (presumed the key derivation is done frequently enough) through the key derivation protocol?

   (b) Assume the Diffie-Hellman key exchange is done with a 1024 bit prime, and the encryption algorithm is triple-DES. Why doesn't it make cryptographic sense to do use the key derivation protocol described above? For your answers, check the paper "Selecting Cryptographic Key Sizes" by Lenstra and Verheul which was a handed out as a reading assignment. Describe the attack that would require the least computational effort from Oscar.

   (c) Assume now that the Diffie-Hellman key exchange is done with a 2048 bit prime, and the encryption algorithm is DES. Does the key derivation strengthen the cryptosystem now? Again, refer to the Lenstra/Verheul paper.

2. People at your new job are deeply impressed that you took and survived EE578/CS578. As the first job assignment you are asked to design a digital pay-TV system which uses encryption for preventing service theft through wire tapping. As key exchange protocol, a strong Diffie-Hellman with, e.g., 2048 bit modulus is being used. However, since your company also wants to export the system, as encryption algorithm only DES is allowed. You decide to use a key derivation approach as described in Equation (1).

   (a) First we have to determine whether the attacker can store an entire movie with reasonable efforts (in particular costs). Assume the data rate for the TV link is 1Mbit/s, and that the longest movies we want to protect are 2h long. How many Gbytes (where $1M = 10^6$ and $1G = 10^9$) of data must be stored for a 2h film (don't mix up bits and bytes here)? Is this realistic?

(b) We assume that an attacker will be able to find a DES key in 10min using a brute-force attack. Note that this is a somewhat optimistic assumption from an attacker's point of view, but we want to provide some medium-term security by assuming increasingly faster key searches in the future.

How frequently must a key be derived if the goal is to prevent an off-line decryption of a 2h movie in less than 30 days?

3. Draw a block digram for the following two hash functions build from block ciphers $e()$:

$$H_i = H_{i-1} \oplus e_{x_i}(H_{i-1}) \quad (2)$$

$$H_i = H_{i-1} \oplus x_i \oplus e_{g(H_{i-1})}(x_i) \quad (3)$$

(The following problem has a simple answer.) Describe why there is no mapping function $g(x_i)$ needed for feeding $x_i$ into the key-input of the block cipher $e()$ in Equation (2).

4. For hash function is is crucial to have a sufficiently large number of output bits, with, e.g., 160 bit, in order to thwart attacks based on the birthday paradox. Why are much shorter output lengths of, e.g., 64 bit, sufficient for MACs?

For your answer, assume a message $x$ that is sent in clear together with its MAC over the channel: $(x, MAC_k(x))$. Exactly clarify what Oscar has to do to "attack" this system.

5. Why does sender (or message) authentication imply data integrity? Is the opposite true too, i.e., does data integrity imply sender authentication? Justify both answers.

6. (a) Assume we apply the integrity techniques described in Subsection XIV.4.3 of the lecture, according to which the ciphertext $c$ is computed as

$$c = e_k(x||H(x))$$

where $H()$ is a hash function. This technique is not suited for encryption with stream ciphers if the attacker knows the whole plaintext $x$. Explain *exactly* how an active attacker can now *replace* $x$ by an arbitrary $x'$ of his/her choosing and compute $c'$ such that the receiver will verify the message correctly. Assume that $x$ and $x'$ are of equal length. Will this attack work too if the encryption is done with a one-time pad?

(b) Is the attack still applicable if the checksum is computed using a keyed hash function such as a MAC:

$$c = e_{k_1}(x||MAC_{k_2}(x))$$

Assume that $e()$ is a stream cipher as above. Exactly motivate your answer, i.e., write more than a "yes" or a "no".