Technische Universität München
Informatik VIII
Netzarchitekturen und Netzdienste
Prof. Dr.-Ing. Georg Carle

Dipl.-Inform. Heiko Niedermayer
Dipl.-Inf. Ali Fessi

Exercises for lecture „Netzsicherheit“
Assignment 2, WS09/10

Hand-out:	Wednesday November 18th 2009
Deadline:	Thursday December 3rd 2009
Exercise course:	Thursday December 10th 2009

Task 1: Meet-In-The-Middle Attack on Double-DES

The encryption algorithm Double-DES is defined as follows: There is a symmetric key K with length 112 bits (2 x 56 bits). This key is divided into two keys: K_1 und K_2. The plaintext P is encrypted by using the different keys on after another:

$$C = E(K_2, E(K_1, P))$$

E is the encryption function of DES.
Do some research on the Internet or check appropriate books. As a result you should describe the Meet-in-the-Middle-Attack on Double-DES, best with some figure.

Argue why Double-DES provides only a little more security than a single DES.

Task 2: Symmetric Encryption in Counter Mode (CTR)

Figure 1 shows how the CTR mode operates.

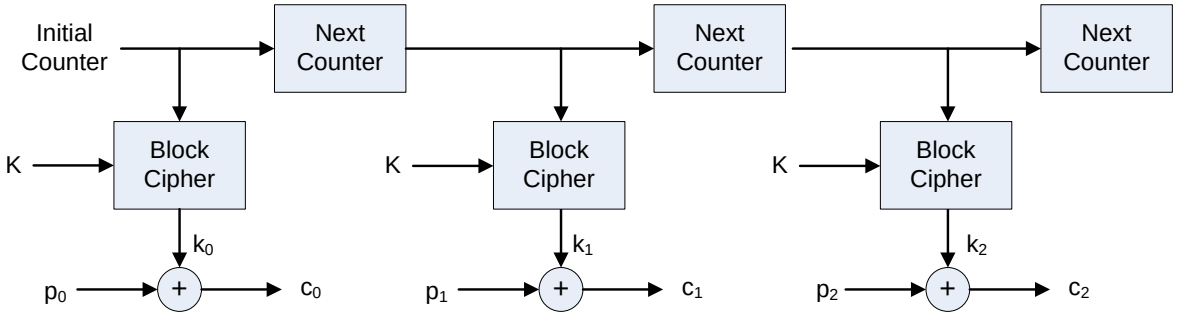

Figure 1: Symmetric Encryption in CTR Mode

a) Describe how an attacker can selectively flip bits of a message encrypted with CTR mode. What can be done to defend such attacks?

b) Now assume that there is a new key stream ($k_0 \| k_1 \| k_2$...) for every new message which is generated from freshly generated "Initial Counter". Why does the reuse of an "Initial Counter" when using the same key K lead to a so-called „Known-Plain-Text Attack"[1].

Task 3: RSA Algorithm

a) Let $n = 11 \times 17 = 187$. Now calculate the number of numbers $m \in \mathrm{N}$, so that $1 \leq m \prec n$ and $\gcd(n, m) = 1$.
b) Let $M = 13$. M is not to be encrypted according to the RSA algorithm. Let the public key be $n = 187$ and the exponent $e = 3$. It is your task to compute the cipher text C for M.
c) The application of the extended euclidian algorithm gives

$$3 \times 107 - 2 \times \Phi(n) = 1$$

The next step is calculate the private key of this RSA application, when the public key is the one of this task with $n = 187$ and $e = 3$.
Now, verify your result using the example message $M = 13$ by showing that the decryption of $C = E(M)$ will result in M.

Task 4: Man-In-The-Middle Attack on RSA and Diffie-Hellmann

a) Let us assume that Bob wants to communicate with Alice. The communication shall be protected with a secure channel to prevent eavesdropping. This secure requires that in every direction there is an encryption with the RSA algorithm. K_{A-pub} and K_{B-pub} are the public keys of Alice and Bob. K_{A-priv} and K_{B-priv} are the private keys. The current state is that neither Bob nor Alice know the public keys of the other communication partner.

Describe the messages that would be exchanged between Alice, Bob, and Mallory, when Mallory does a Man-In-The-Middle attack (MITM).

b) Now assume that Alice and Bob want to exchange a shared secret key using Diffie-Hellman.. Describe the messages that would be exchanged between Alice, Bob, and the attacker Mallory when Malory does a Man-In-The-Middle attack. With whom do the participants have exchanged a shared key in that case?

Task 5: Message Authentication Codes

The standard HMAC (HMAC: Keyed-Hashing for Message Authentication) is defined in RFC 2104, see http://www.ietf.org/rfc/rfc2104.txt.

a) Read the abstract and determine if the HMAC operation is bound to a certain cryptographic hash function?
b) Read the section on „Definition of HMAC" . Please provide and describe the HMAC formula.
c) What are other possible MAC function that you know from the lecture? Give one example.
d) Can MAC functions be used for digital signatures? Justify your answer.

[1] A "Known-Plain-Text Attack" can happen when an attacker has one or multiple message pairs (P_i, C_i) and it can as a consequence decrypt C_j. It is possible that the attacker simply guesses the content of messages or that is only knows parts of the messages. P_i may also only be revealed in parts or one may have had to guess.