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

Dipl.-Inform. Ralph Holz

Exercises for lecture „Netzsicherheit“
Assignment 2, WS10/11

Hand-out:	Thursday November 04th 2010
Deadline:	Thursday November 11th 2010
Exercise course:	Wednesday November 17th 2010

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

DES is the Data Encryption Standard, a symmetric cipher. Unfortunately, the keylength, as specified in the standard, is too short for today's strong computers. That is why 3DES, a triple application of DES, is sometimes used. Double-DES, however, is not an option. In this exercise, you'll find out why.

Double-DES can be defined as follows. There is a symmetric key K with length 112 bits (2 x 56 bits). This key is divided into two halves: K_1 und K_2. The plaintext P is encrypted by using the two halves as single keys in one DES encryption after the other. We thus obtain the ciphertext C:

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

E is the encryption function of DES.

Unfortunately, there is a practical attack on Double-DES: Meet-In-The-Middle. Do some research on the Internet or in relevant cryptographic literature (books, scripts etc). You'll find some help here: http://www-dm.informatik.uni-tuebingen.de/lehre/kryptoVL/ws1011/Literatur.pdf

Then answer the following questions:

- How does the Meet-in-the-middle attack on Double-DES work? Explain the principle. Which computing resource is traded against which?
- In terms of key length, how secure is Double-DES compared to normal DES?

Task 2: Symmetric Encryption in Counter Mode (CTR)

Figure 1 shows how the CTR mode operates.

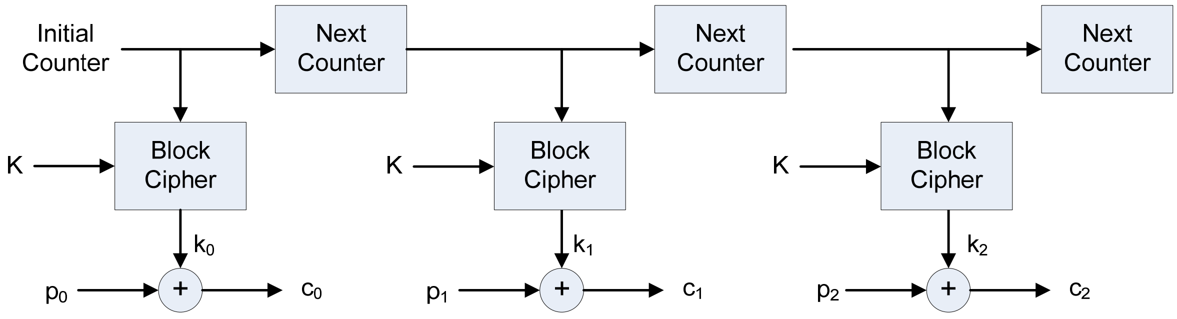

Figure 1: Symmetric Encryption in CTR Mode

a) CTR mode is popular with AES. Why? But what are the disadvantages of CTR mode?
b) Assume that a transmission error occurs and several consecutive bits (of the same block) in the ciphertext are flipped. When decrypting the ciphertext, which bits will be affected in the decrypted plaintext?
c) A cipher mode's reaction to flipped bits – i. e. the extent to which it lets errors propagate – is called its "fault tolerance". Compare the fault tolerance of CTR mode with the one of CFB mode.
d) Assume CTR mode is used in streaming data, but synchronisation between the two communication endpoints is lost. Can it be recovered without external mechanisms? Why? Can it be recovered with CFB?
e) In a Known-Plain-Text Attack, an attacker already has one or multiple plaintext/ciphertext pairs (p_i, c_i)[1]. This sometimes allows him to break other ciphertexts as well.
With CTR mode, the initial counter is usually different for each new communication. However, assume now that we are a bit careless and *reuse it while also using the same key K.* Also assume that the attacker fulfils the prerequisites of a Known-Plaintext Attack and already has a pair of plaintext and ciphertext (p_i, c_i) from a previous communication (with same initial counter and key). Show how this reuse allows a successful Known-Plain-Text Attack.

Task 3: RSA Algorithm

We will practice the RSA algorithm here.

a) Let $n = 11 \times 17 = 187$. Now calculate the number of numbers $m \in \mathrm{N}$, so that $1 \le m \prec n$ and $\gcd(n, m) = 1$.
b) Let $M = 13$. M is now to be encrypted according to the RSA algorithm. Let the public key be $n = 187$ and the exponent $e = 3$. 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 before, 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

Let us now have a look at so-called Man-in-the-middle attacks (MITM). If you haven't already done so, do some research on the principles of this attack.

a) Let us assume that Bob (B) wants to communicate with Alice (A) over an unsecured channel. Both have RSA key pairs: $K_{A,pub}$ and $K_{B,pub}$ shall be the public keys, and $K_{A,priv}$ and $K_{B,priv}$ are the private keys. However, the public keys have not been exchanged yet. Explain why they cannot establish an encrypted channel. Denoting the attacker by Mallory (M), sketch how M can act as a MITM (draw figures, if it's easier to explain).

b) Now assume that Alice and Bob want to agree on a shared secret key. They have heard about the Diffie-Hellman scheme, but have not understood its implications. Mallory is the evil attacker again and does a MITM attack. Describe the messages that would be exchanged between Alice and Bob, and show how Mallory can interfere. What are the thus established keys that Alice, Bob and Mallory have after the scheme?

[1] This can, e. g., happen if the attacker can simply guess the content of messages. It is not too unlikely in certain cases, e. g. `HTTP GET index.html` (or in an SMS: `CU tomorrow`).

c) The MITM attacks from above were trivial, in the sense that (hopefully) no one would attempt to do it this way. In practice, what can be done to make asymmetric encryption and Diffie-Hellman secure schemes? Describe two possibilities.

Task 5: Message Authentication Codes

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

a) Read the abstract. Is the HMAC operation bound to a certain cryptographic hash function?
b) Read the section on „Definition of HMAC“. Explain the steps of the HMAC formula.
c) What are further possible MAC functions that you know from the lecture? Give at least one example.
d) Can MAC functions also be used for digital signatures? Justify your answer. What is the goal of a digital signature compared to a MAC?