Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

Tutorial 6

Friday, December 4, 2015

Problem 1. *(Blum-Blum-Shub generator)* The security of the Blum-Blum-Shub generator is based on the difficulty to compute square roots modulo $n = pq$ for two distinct primes p and q with $p, q \equiv 3 \mod 4$.

Design a generator for pseudo-random bits which is based on the hardness of the RSA-problem.

Problem 2. *(number of messages and hardware resources of two hash functions)* Consider two hash functions, one with an output length of 64 bits and another one with an output length of 128 bits.

For each of these functions, do the following:

a) Determine the number of messages that have to be created to find a collision with a probability larger than 0.86 by means of the birthday paradox.

b) Determine the hardware ressources required for this attack in terms of memory size, number of comparisons, and number of hash function executions.

Problem 3. *(CBC and CFB for MAC generation)* Both, the CBC mode and the CFB mode, can be used for the generation of a MAC as follows.

- A plaintext is divided into n equally-sized blocks $M_1, ..., M_n$.
- For the CFB-MAC, the ciphertexts are $C_i = M_{i+1} \oplus E_K(C_{i-1})$ for $i = 1, \ldots, n-1$ and $\mathrm{MAC}_K^{(n)} = E_K(C_{n-1})$ with initial value $C_0 = M_1$.
- For the CBC-MAC, the ciphertexts are $\hat{C}_i = E_K(\hat{C}_{i-1} \oplus M_i)$ for $i = 1, \ldots, n-1$ and $\widehat{\mathrm{MAC}}_K^{(n)} = E_K(\hat{C}_{n-1} \oplus M_n)$ with initial value $\hat{C}_0 = 0$.

Show that the equivalency $\mathrm{MAC}_K^{(n)} = \widehat{\mathrm{MAC}}_K^{(n)}$ holds.

Problem 4. *(derive a message validation protocol)* Suppose Alice transmits the following cryptogram to Bob:

$$c = e(m \parallel h(k_2 \parallel m), k_1).$$

Assume that the message m, the shared keys k_1, k_2, the hash values $h(x)$ and the output of the encryption function have fixed lengths known to Alice and Bob.

a) Derive a protocol for decryption and message validation used by Bob.

b) Modify the given scheme to construct a similar protocol for a public-key cryptosystem. You may use two private-/public key-pairs (K_1, L_1) and (K_2, L_2) and a session key s used in the hash, which is securely transmitted to Bob within the cryptogram c.

c) How can an intruder Eve impersonate Alice to Bob in the system of (b)? How could the attack be prevented?