CHALMERS TEKNISKA HÖGSKOLA
Datavetenskap
Björn von Sydow INN150/TDA350

Solutions to exam in Cryptography 061217

1. (a) Message length is $8 \cdot 25 = 200$ bits. The period length for an LFSR with size L bits is at most $2^L - 1$. To achieve a period of at least 200 bits we must thus choose $L \geq 8$. The LFSR size is also the size of the key (the initial content), so minimum key size is 8.

   (b) The adversary can construct the first 40 bits of the message m and thus determine the first 40 bits of the keystream (as $b = c \oplus m$). But to completely determine the tap sequence of an 8 bit LFSR it is enough to know $2 \cdot 8 = 16$ consecutive bits of output. So the adversary can decrypt Alice's messages.

2. (a) We can rewrite the two given equations as follows. We swap left and right hand sides in both equations; in the second we xor both sides with $f(K_i, R_i)$ to get

$$\begin{aligned} R_i &= L_{i+1} \\ L_i &= R_{i+1} \oplus f(K_i, R_i). \end{aligned}$$

   Finally, we replace the last occurrence of R_i with L_{i+1}. The resulting equations show how to compute $L_i||R_i$ from $L_{i+1}||R_{i+1}$. Thus round i is invertible, regardless of f. The same reasoning holds for all rounds, so no conditions need to be imposed on f (except, of course, that it takes input and produces output of appropriate sizes).

   (b) Decryption is the same operation as encryption except for subkey order, which is reversed in decryption.

3. (a) Mallory's assumption is that Alice's message is $10x$ for some integer x. Then we have $c = (10m)^e = 10^e m^e$, where the computations are in $\mathbb{Z}_N^*$. Mallory can compute 10^e and invert it using the extended Euclidean algorithm to get 10^{-e}. Finally, he constructs the bid $c \cdot (10)^{-e} \cdot 11^e$, which equals $(11m)^e$, i.e. the encryption of $11m$.

   (b) Two main ingredients in padding are randomization (to avoid that the same message encrypted twice gives the same encryption) and redundancy (so that randomly constructed ciphertexts are unlikely to be encryptions of a valid message).

4. (a) The hash function h is collision resistant if it is infeasible to find two different messages m_1 and m_2 with $h(m_1) = h(m_2)$.

   (b) First the message is hashed and then the signature is applied only to the hash value.

   (c) A MAC takes as input both a message and a secret key, while a hash function takes only a message as input.

(d) Because of the birthday attack, collisions for a hash function with hash values of size $2n$ bits can be found in $O(2^n)$ steps. Thus, if overall security should be n bits, corresponding to $O(2^n)$ steps for the best known attack, hash values of size $2n$ gives the desired security.

5. The remainder of the run is as follows:

$$\begin{array}{lcl} 4. \quad B \longrightarrow C(T) & : & \{A, N_B\}_{K_{BT}}. \\ 5. \quad C(T) \longrightarrow B & : & \{A, N_B\}_{K_{BT}}. \end{array}$$

Note that when receiving message 3, B expects an encrypted value that he will just pass on to T. He therefore does so, in particular without noticing that what he got back was in fact his nonce unencrypted.

So, when C intercepts message 4, he can return it unchanged to B, without need to decrypt and reencrypt anything, as the protocol intends. When B receives the message he follows the instructions, checks Alice's identity and the nonce and accepts the run.

6. (a) Following the problem text, the adversary has received $m = E_k(x \oplus C_0)$ and $t = E_k(m \oplus C_0)$. But now consider the two-block message $x||C_0$. The CBC encryption of this message is $m||t$, and thus its MAC is t. So, the adversary can construct this message/MAC pair and win the game.

(b) If the encryption of message $x = x_1 x_2 \ldots x_n$ is $c_1 c_2 \ldots c_n$, then the MAC is c_n. Thus the last block of the complete ciphertext (including the encryption of the MAC) is thus $E_k(c_n \oplus c_n) = E_k(0)$, which is independent of the message.

The consequence is that the MAC becomes useless. Its purpose is to authenticate the message, ensuring the intended receiver that the message has not been tampered with. But from just eavesdropping to one MAC:ed message, the adversary can use the last block as a MAC to any ciphertext he chooses.

7. The formulas for computing the x_k show that $x_s = (x_0)^{2^s} = a^{m \cdot 2^s} = a^{n-1} = 1$, where the last equality is by Fermat's theorem. So, if $x_0 \neq 1$, there must be some $k < s$ such that $x_k \neq 1$ and $x_k^2 = x_{k+1} = 1$. But this means that x_k is a square-root of 1 different from 1. If n is a prime, the only square-roots of 1 in $\mathbb{Z}_n^*$ are 1 and $n-1$, since $x^2 = 1 \bmod n$ is equivalent to $(x-1)(x+1) = 0 \bmod n$, which implies $x - 1 = 0 \bmod n$ or $x + 1 = 0 \bmod n$. Hence we must have $x_k = n - 1$.