CHALMERS TEKNISKA HÖGSKOLA
Datavetenskap
Björn von Sydow INN150/TDA350/TDA351

Solutions to exam in Cryptography 081218

1. Period is 7, so the length must be at least 3. Let the tap sequence be $c_1c_2c_3$. From the given output sequence we can form the system of equations

$$\begin{aligned} 0c_1 \oplus 0c_2 \oplus 1c_3 &= 1 \\ 1c_1 \oplus 0c_2 \oplus 0c_3 &= 1 \\ 1c_1 \oplus 1c_2 \oplus 0c_3 &= 1. \end{aligned}$$

   This is directly solved from top to bottom, giving $c_3 = 1$, $c_1 = 1$, $c_2 = 0$.

   We also need to check that this LFSR actually produces the given output, i.e. that the seventh bit of output is 0. Since we tap at positions 1 and 3, the seventh bit is $1 \oplus 1 = 0$.

2. (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) We should expect to get a collision in $O(2^{n/2})$ steps; this is the so-called birthday "paradox".

3. (a) Let $c = DESX_{(k_1,k_2)}(m)$. We first xor both sides with k_2, which gives $c \oplus k_2 = DES_{k_1}(m \oplus k_2)$. Next, we apply DES decryption, to get $DES_{k_1}^{-1}(c \oplus k_2) = m \oplus k_2$. Finally, we again xor both sides with k_2 to get the final result

$$m = DES_{k_1}^{-1}(c \oplus k_2) \oplus k_2.$$

   (b) This cipher can be attacked using a meet-in-the-middle attack. We assume that the adversary has a few plaintext/ciphertext pairs (m, c). He can then do a brute force attack on the DES part, i.e. compute $x = DES_{k_1}(m)$ for all possible keys k_1, and store the resulting pairs (x, k_1) in a dictionary. Then he goes through all possible k_2, computes $c \oplus k_2$ and looks it up in the dictionary. When found, he has a potential key pair (k_1, k_2). The complexity of this attack is 2^{64}, which shows that the cipher does not provide 120 bits of security.

   Alternatively, with two plaintext/ciphertext pairs (m_1, c_1) and (m_2, c_2), one notes that $c_1 \oplus c_2 = DES_{k_1}(m_1) \oplus DES_{k_1}(m_2)$, which makes it possible to do a brute force attack with only twice the cost of an attack against DES.

4. (a) No. We require that $ed = 1 \bmod \Phi(N)$, where d is the decryption exponent. But $\Phi(N) = (p-1)(q-1)$ is an even number, so if e is even, we cannot find such a d.

(b) The adversary has eavesdropped and thus knows $c = m^e$ and $c' = m^{e'}$. He also knows e and e'. Furthermore, $\gcd(e, e') = 1$, since $e' = e + 2^i$ for some i. (Any non-trivial divisor of e must be odd, hence not a divisor of 2^i, hence not a divisor of e'.) So the adversary can find integers x and y such that $ex + e'y = 1$. Hence

$$c^x \cdot c'^y = m^{ex+e'y} = m.$$

5. (a) Let $C_0C_1C_2C_3$ be message 2 in a run of the protocol. Then $C_1C_2C_3$ is a valid CBC mode encryption of N_AN_B, so if the order were not changed, an adversary could complete the protocol by just stripping the first block, without knowing K_{AB}.

   (b) The adversary starts a run of this protocol, using B as nonce, i.e. the beginning of the protocol is

$$\begin{array}{lll} 1.\ \ C(A) \to B & : & A, B \\ 2.\ \ B \to A & : & \{A, B, N_B\}_{K_{AB}} \end{array}$$

   If, again, $C_0C_1C_2C_3$ is message 2, then the adversary can strip the last block from this to get a valid CBC mode encryption of A, B.

6. (a) Victor checks that $R \cdot S = X$ (since $R \cdot S = g^{r+(x-r)} = g^x = X$) and either $R = g^z$ (if $b = 0$) or $S = g^z$ (if $b = 1$).

   (b) If the false Peggy guesses that she will get $b = 0$ in message 2, she chooses r at random, and sends $R = g^r$, $S = R^{-1}X$. Her values will then pass Victor's check. If she guesses that $b = 1$, exchange R and S. In both cases, $z = r$.

   (c) Repeat the protocol t times and accept only if the check succeeds each time. Then a false Peggy has probability 2^{-t} to be accepted.

7. (a) To decrypt ciphertext (Y, c) encrypted for a user with private key x, we proceed as follows:
   - Compute $K = Y^x$ (this will be the same as X^y, computed by the sender).
   - Compute $k = b(K)$, where the length of k is the length of c.
   - Compute $z = c \oplus k$ and parse this as $m||t$, where t is n bits long.
   - Compute $H(m)$; if this equals t, then return m, else decryption fails.

   (b) The adversary gets the ciphertext (Y, c'). He then asks for decryption of

$$(Y, c' \oplus (m_0||H(m_0)) \oplus (m_1||H(m_1))).$$

   If we plug in what c' is, we see that the message the adversary constructs is a valid encryption of the *other* message, i.e. the message that Alice did not pick. After getting the decryption, he knows which message Alice did pick.

   (c) We just replace the subgroup G with an elliptic curve group. Computations Y^x and X^y will be replaced by multiplications by a scalar. We have also to agree on some way to use a point as seed to the bit generator e.g. by using the x-coordinate.

   The advantage is that we can use much smaller keys and get more efficient computations for the same level of security.