Cryptography

Problem set 3 - 3-7 IV 2017

Problem 1 Show that the CBC mode of encryption does not yield CCA-secure encryption scheme regardles of F.

Problem 2 Show that the OFB mode of encryption does not yield CCA-secure encryption scheme regardles of F.

Problem 3 Show that the counter mode of encryption does not yield CCA-secure encryption scheme regardles of F.

Problem 4 Consider a variant of CBC where in each encryption IV is increased by 1 (instead of choosing it at random). Show that the variant is not CPA-secure.

Problem 5 (2 points) Let $F : \{0,1\}^n \to \{0,1\}^m$ be a function. We say that F behaves as linear function if there exists $i_1, \ldots, i_k \in \{1, \ldots, n\}$ and $j_1, \ldots, j_l \in \{1, \ldots, m\}$ such that

$$P(*) = P(X_{i_1} \oplus \ldots \oplus X_{i_k} = Y_{i_1} \oplus \ldots \oplus Y_{i_j})$$

and $|P(*) - 1/2|$ is non-negligible. The probability is taken over all possible values of X where $F(X) = F(X_1 X_2 \ldots X_n) = Y_1 \ldots Y_m$.

Consider F as:

- a random function (consider both $n = m$ and $n \neq m$),
- a random permutation.

Evaluate $|P(*) - 1/2| \geq 1/d$, for $d = 3, 4, \ldots$?

Problem 6 Compute the expected number of (single) collisions after q queries to a Random Oracle which returns binary strings of length n (*i.e.,* compute the number of pairs $i, j \in \{1, \ldots, q\}$ where $i \neq j$ and $h(x_i) = h(x_j)$).

Problem 7 Let p and $q = (p-1)/2$ be primes. Let α, β be two primitive roots for p. Let $\alpha^a \equiv \beta (\mathrm{mod} p)$. We define the hash $h : \{0, \ldots, q^2 - 1\} \to \{0, \ldots, p-1\}$ as follows: for $m = x_0 + qx_1$ (for $0 \leq x_0, x_1 \leq q-1$) let:

$$h(m) = \alpha^{x_0} \beta^{x_1} (\mathrm{mod} p).$$

Show that h is collision-free. (Hint: show that if one can find $m \neq m'$ such that $h(m) = h(m')$ then one can determine the discrete logarithm $a = \log_\alpha \beta$.)

Problem 8 Show how to get possible round keys from a three-round SP-network. You can assume that you know m pairs of the corresponding plaintext-ciphertext pairs. You can assume that each S-box has 4-bit input and 4-bit output and that the whole SP-network encrypts 64-bit messages (so there are 16 S-boxes). What is the complexity of the attack if 64-bit block is replaced with 128-bit block and each S-box has 8-bit input and output?

Problem 9 Show that selecting S-boxes at random for an SP-network is not a good idea. Show that for randomly selected S-box linear attacks will be possible.