Cryptography

Problem set 4 - 7-8 IV 2015

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 Show that *encrypt-and-authenticate* transformation – $\langle c, t\rangle$ is not necessarily CCA-secure:

$$c \leftarrow \mathsf{Enc}_{k_1}(m) \quad t \leftarrow \mathsf{Mac}_{k_2}(m)$$

even if encryption scheme $\langle \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}\rangle$ is CPA-secure and MAC scheme $\langle \mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy}\rangle$ is unforgeable.

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 $d = 3, 4, \ldots$?