Cryptography Midterm Exam

Problem 1 [12pt]. For each of the following statements below, determine whether it is true or false. Justify your answers.

(a) (2pt) A stream cipher has perfect secrecy.
(b) (2pt) Suppose that $G : K \to \{0,1\}^n$ is a PRG such that $\bigoplus_{i=1}^{n} G(k)[i] = 1$ where $G(k)[i]$ is the i-th bit. Then G is predictable.
(c) (4pt) Let $X = \{0,1\}$. Consider the following PRP $F : \{0,1\} \times \{0,1\} \to \{0,1\}$ defined by $F(k,x) := k \oplus x$. Then F is not a secure PRP.
(d) (4pt) Let $I = (S,V)$ be a MAC. Suppose that an attacker is able to find $m_0 \neq m_1$ s.t. $S(k,m_0) = S(k,m_1)$ for half of the keys in K. Then this MAC is secure.

Problem 2 [22pt]. Show that the required time and memory of the Baby-step & Giant-step algorithm for solving Discrete Logarithm Problem (DLP) are $O(\sqrt{n})$.

Problem 3 [21pt].

(a) (7pt) Let $G : \{0,1\}^s \to \{0,1\}^n$ be a secure PRG. Prove or disprove that $H(k) = rev(G(k))$ is a secure PRG, where $rev(x)$ reverses the string x so that the first bit of x is the last bit of $rev(x)$, the second bit of x is the second to last bit of $rev(x)$, and so on.
(b) (7pt)Let $G : \{0,1\}^n \to \{0,1\}^{n+1}$ be a secure PRG. Define $H(x_1 \| x_2) = G(x_1) \| G(x_2)$. Prove or disprove that H is a secure PRG.
(c) (7pt) Let $G : \{0,1\}^s \to \{0,1\}^n$ and $H : \{0,1\}^s \to \{0,1\}^n$ be efficient functions. Define $K : \{0,1\}^s \to \{0,1\}^n$ by $K(m) = G(m) \bigoplus H(m)$. Prove or disprove that K is a PRG if $G(\cdot)$ and $H(\cdot)$ are PRGs.

Problem 4 [15pt]. Prove that two input/output pairs of DES encryption are enough for exhaustive key search by showing the following statement: Given two DES pairs $(m_1, c_1 = \text{DES}(k, m_1)), (m_2, c_2 = \text{DES}(k, m_2))$, for all m, c, there is at most one key k such that $c = \text{DES}(k, m)$ with prob. $\geq 1 - 1/2^{71}$.

Problem 5 [10pt]. Let m be a message consisting of ℓ AES blocks (say $\ell = 50$). Alice wanted to encrypt m using ECB or CBC modes (as in the Figures 1, 2 with $E(k,\cdot) = \text{AES}$) and transmit the resulting ciphertext to Bob. Suppose that one ciphertext block was transmitted incorrectly due to a network error (i.e., some ones are inadvertently changed to zeroes and vice versa). Show that the number of plaintext blocks that will be decrypted incorrectly is equal to one if ECB mode was used for encryption; and equal to two if CBC mode was used.

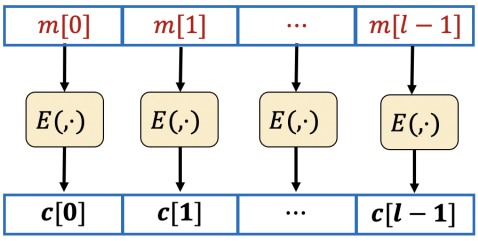

Fig. 1: ECB encryption mode.

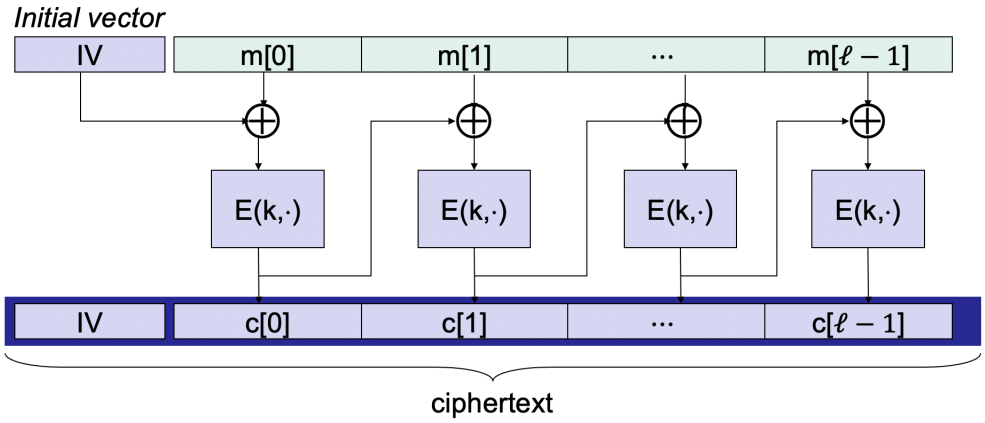

Fig. 2: CBC encryption mode.

Problem 6 [10pt]. Let $F : K \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF. Let $I = (S, V)$ be a secure MAC over $(K', M, T = \{0,1\}^n)$. Define a signing algorithm $\tilde{S}$ such that

$$\tilde{S}((k_1, k_2), m) := (r, F(k_1, r) \oplus S(k_2, m))$$

for $k_1 \leftarrow K, k_2 \leftarrow K'$, $r \leftarrow \{0,1\}^n$. Construct a verification algorithm $\tilde{V}$, so that $\tilde{I} = (\tilde{S}, \tilde{V})$ is a MAC defined over $(K \times K', M, \{0,1\}^{2n})$.

Problem 7 [10pt]. Recall that the ECBC-MAC uses a fixed IV (in the lecture we simply set the IV to 0). Suppose instead we chose a random IV for every message being signed and include the IV in the tag as shown in Figure 3. In other words, $S(k, m) := (r, \text{ECBC}_r(k, m))$ where $\text{ECBC}_r(k, m)$ refers to the ECBC function using r as the IV. The verification algorithm V given key k, message m, and tag (r, t) outputs 1 if $t = \text{ECBC}_r(k, m)$ and outputs 0 otherwise. Show that the resulting MAC system is insecure by a 1-chosen message attack.

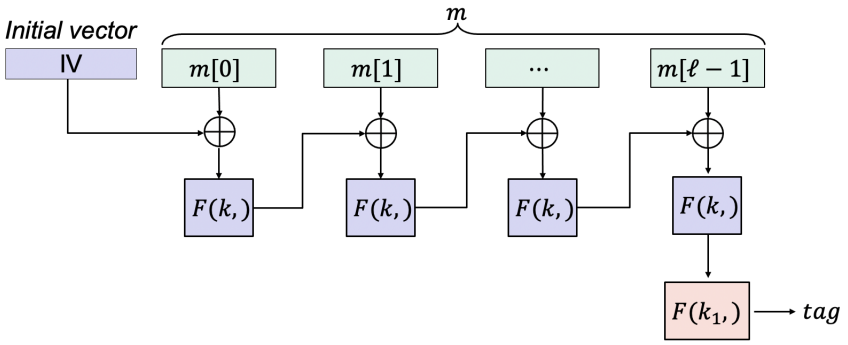

Fig. 3: ECBC-MAC.