Cryptology: Assignment 1

Topics: Classical Ciphers, Perfect Secrecy

1. If an encryption function Enc_K is identical to the decryption function Dec_K, then the key K is said to be involutary. Suppose $K = (a, b)$ be a key in an Affine cipher over $\mathbb{Z}_n$. Prove that K is an involutary key if and only if $a^{-1} \mod n = a$ and $b(a+1) \equiv 0 \mod n$.

2. Show that the Shift, Substitution, and Vigenère ciphers are all trivial to break using a *chosen-plaintext attack*. How many known plaintext is needed to completely recover the key for each of the ciphers (without resorting to any statistics)?

3. Kathakali has intercepted two ciphertexts:

$$c_1 = 111110010111100111001100000101111000011 0\,,$$

$$c_2 = 111110100110011111011101000010011000 1000.$$

   She knows that both are OTP ciphertexts, encrypted with the same key. In addition, she also knows that either c_1 is an encryption of "alpha" and c_2 is an encryption of "bravo" or c_1 is an encryption of "delta" and c_2 is an encryption of "gamma" (all converted to binary from ascii in the standard way).

   Is it possible for Kathakali to deduce which of these two possibilities is correct, and what is the underlying key k?

4. Pritam claims that an encryption scheme with message space $\mathcal{M}$ is perfectly secret if and only if for every probability distribution over $\mathcal{M}$ and every $c_0, c_1 \in \mathcal{C}$, we have

$$\mathsf{Pr}[C = c_0] = Pr[C = c_1].$$

   Is Pritam correct? Justify your answer.

5. Susmita defines the following encryption scheme:

   - $\mathcal{M} = \mathcal{C} = \{0, \ldots, 4\},\ \mathcal{K} = \{0, \ldots, 5\}$.
   - Gen: Returns a key $k \leftarrow_{\$} \mathcal{K}$.
   - $\mathsf{Enc}(k, m)$: Returns $[k + m \mod 5]$.
   - $\mathsf{Dec}(k, c)$: Returns $[c - k \mod 5]$.

   Does the above encryption scheme defined by Susmita achieve perfect secrecy?

6. Prove or disprove (giving one counter example) the following statements about perfect secrecy for symmetric-key encryption.

   (a) There is a perfectly secret encryption scheme for which the ciphertext always reveals 90% of the bits of the key k to the adversary.

   (b) There is an encryption scheme that is not perfectly secure, yet the adversary cannot guess the key with probability greater than $1/|\mathcal{K}|$.

7. Let us consider Π to be a Vigenère cipher where the message space consists of all 3-character strings (over the English alphabet), and the key is generated by first choosing the period t uniformly from $\{1, 2, 3\}$ and then letting the key be a uniform string of length t.

   (a) Monali defines an adversary $\mathcal{A}$ as follows:

   - $\mathcal{A}$ sends two plaintexts $m_0 = aab$ and $m_1 = abb$ to the challenger.
   - Given a ciphertext c, $\mathcal{A}$ outputs 0, if and only if the first character of c is the same as the second character of c.

   Does the adversary defined by Monali demonstrates that the cipher is not perfectly secure? [Hint: Compute $\mathsf{Pr}[\mathsf{Priv}_{\mathcal{A},\Pi} = 1]$].

   (b) Can you construct an adversary $\mathcal{A}'$ for which $\mathsf{Pr}[\mathsf{Priv}_{\mathcal{A}',\Pi} = 1]$ is greater than the one constructed by Monali?

8. Let $\epsilon \geq 0$ be a constant. Dipan defines a new notion of perfect secrecy as follows: an encryption scheme to be ϵ-perfectly secret if for every adversary $\mathcal{A}$ it holds that

$$\mathsf{Pr}[\mathsf{Priv}_{\mathcal{A},\Pi} = 1] \leq \frac{1}{2} + \epsilon\,.$$

   Dipan claims that

   (a) ϵ-perfect secrecy can be achieved with $|\mathcal{K}| < |\mathcal{M}|$, when $\epsilon > 0$.

   (b) $|\mathcal{K}| < (1 - 2\epsilon) \cdot |\mathcal{M}|$.

   Justify the validity of Dipan's claims.