Cryptography and Security 2017

Exercise Sheet 3

Exercise 1 Vigenère Cipher

We formalize the Vigenère Cipher as follows:

- Let $\mathsf{A} = \mathbf{Z}_{26}$ denote the alphabet, A^* denotes the set of all finite sequences (or *strings*) of elements in A. For $s \in \mathsf{A}^*$ we denote by $|s|$ its length and s_i its ith element for $i = 0, 1, \ldots, |s| - 1$.
- The plaintext space, key space, and ciphertext space are A^*.
- We assume that given a random plaintext $X = (X_0, \ldots, X_{n-1})$ of length n, all X_i are independent with distribution p. That is

$$\Pr\left[X = x \,\middle|\, |X| = n\right] = \prod_{i=0}^{n-1} p(x_i)$$

- We assume that given a key $K = (K_0, \ldots, K_{k-1})$ of length k, all K_i are independent and follow a uniform distribution. That is

$$\Pr\left[K = \kappa \,\middle|\, |K| = k\right] = \frac{1}{26^k}$$

- The ciphertext Y is defined by

$$Y_i = X_i + K_{i \bmod k} \bmod 26$$

for $i = 0, 1, \ldots, n - 1$.

1. Given a string s, we define the index of coincidence $I_c(s)$ as the probability that two elements of s selected at random at different positions are equal. Given $c \in A$, let $n_s(c)$ be the number of index positions i such that $s_i = c$. Show that

$$I_c(s) = \sum_{c \in A} \frac{n_s(c)(n_s(c) - 1)}{|s|(|s| - 1)}$$

2. Let X be a random plaintext of length $n = |X|$. Express the expected value $I_p = E(I_c(X))$ in terms of n and p.

   - We denote I_u the value of I_p when p is the uniform distribution.
     Deduce I_u from the previous question.

3. Let $n = qk + r$ be the Euclidean division of n by k. We pick I and J different with uniform distribution and let $\mathcal{E}$ be the event that $I \bmod k = J \bmod k$.

   - Show that $\Pr[Y_I = Y_J | \neg\mathcal{E}] = I_u$.
   - Show that $\Pr[Y_I = Y_J | \mathcal{E}] = I_p$.
   - Show that

$$\Pr[\mathcal{E}] = \frac{q(2n - k(q + 1))}{n(n - 1)}$$

   - Deduce the value $E(I_c(Y))$.
   - Using $n \gg 1$, $q \approx \frac{n}{k}$ and $E(I_c(Y)) \approx I_c(Y)$, deduce a formula to estimate k based on $I_c(Y)$.

Exercise 2 Vernam with Two Dice

Our crypto apprentice decided to encrypt messages $x \in \mathbf{Z}_{12}$ (instead of bits) using the generalized Vernam cipher in the group $\mathbf{Z}_{12}$. As he did not fully understand the course, he decided to pick a key k (for each x) by rolling two dice (with 6 faces numbered from 1 to 6) and setting $k = k_1 + k_2$ to the sum of the two faces up k_1 and k_2. The encryption of x with key k is then $y = (x + k) \bmod 12$.

1. Why is this encryption scheme insecure?

2. We still use $k = k_1 + k_2$. Given a factor n of 12, we now take $x \in \mathbf{Z}_n$ and $y = (x+k) \bmod n$. Show that for some values n, this provides perfect secrecy but for others, this does not. (Consider *all* factors n of 12.)

3. Finally, the crypto apprentice decides to encrypt a bit $x \in \{0, 1\}$ into $y = (x + k) \bmod 4$, still with $k = k_1 + k_2$ from rolling the two 6-face dice. We assume that x is uniformly distributed in $\{0, 1\}$. For each c, compute the probabilities $\Pr[x = 0|y = c]$ and $\Pr[x = 1|y = c]$.

4. By taking $\tilde{x} \in \{0, 1\}$ as a function of c such that $\Pr[x = \tilde{x}|y = c]$ is maximal, compute the probability $P_e = \Pr[x \neq \tilde{x}]$ (still when x is uniform in $\{0, 1\}$).