Cryptography and Security 2017

Solution Sheet 3

Solution 1 Vigenère Cipher

1. We pick two index positions I and J at random such that they are different. That is, for any i and j such that $i \neq j$ we have $\Pr[I = i, J = j] = \frac{1}{|s|(|s|-1)}$. We have $I_c(s) = \Pr[s_I = s_J] = \sum_{c \in A} \Pr[s_I = s_J = c]$. Now, $\Pr[s_I = s_J = c]$ is $\frac{n_s(c)(n_s(c)-1)}{|s|(|s|-1)}$ so we obtain the formula.

2. We have $n_s(c) = \sum_{i=0}^{n-1} 1_{X_i=c}$ so $E(n_s(c)) = np(c)$. Similarly, we have $n_s(c)^2 = \sum_{i,j=0}^{n-1} 1_{X_i=X_j=c}$. If $i = j$, we have $E(1_{X_i=X_j=c}) = p(c)$. If $i \neq j$, we have $E(1_{X_i=X_j=c}) = p(c)^2$. So, $E(n_s(c)^2) = np(c) + n(n-1)p(c)^2$. By linearity of E, we thus obtain

$$I_p = E(I_c(X)) = \sum_{c \in A} p(c)^2$$

$I_u = \frac{1}{26}$

3. - We have $E(I_c(Y)) = \Pr[Y_I = Y_J]$ where the probability holds over the distribution of I, J, X, and K. Clearly,

$$\Pr[Y_I = Y_J | \neg\mathcal{E}] = \Pr[X_I + K_{I \bmod k} \equiv X_J + K_{J \bmod k} \pmod{26} | \neg\mathcal{E}] = I_u$$

   since $K_{I \bmod k}$ and $K_{J \bmod k}$ are independent and uniformly distributed.

   - We have

$$\begin{aligned}\Pr[Y_I = Y_J | \mathcal{E}] &= \Pr[X_I + K_{I \bmod k} \equiv X_J + K_{J \bmod k} \pmod{26} | \mathcal{E}] \\ &= \Pr[X_I = X_J | \mathcal{E}]\end{aligned}$$

   since $K_{I \bmod k} = K_{J \bmod k}$. We split this probability over all possible values of $I \bmod k$. In each case, we obtain something which is I_p on average since all plaintext elements are independent. Thus, $\Pr[Y_I = Y_J | \mathcal{E}] = I_p$.

   - For $i = 0, 1, \ldots, r-1$, we have $\Pr[I \bmod k = J \bmod k = i] = \frac{(q+1)q}{n(n-1)}$. For $i = r, r+1, \ldots, k-1$, we have $\Pr[I \bmod k = J \bmod k = i] = \frac{q(q-1)}{n(n-1)}$. Thus,

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

   - By collecting all previous results we have

$$E(I_c(Y)) = I_p \Pr[\mathcal{E}] + I_u(1 - \Pr[\mathcal{E}]) = (I_p - I_u)\Pr[\mathcal{E}] + I_u$$

   Using the expression of $\Pr[\mathcal{E}]$ we finally obtain

$$E(I_c(Y)) = (I_p - I_u)q\frac{2n - k(q+1)}{n(n-1)} + I_u$$

   - We have

$$I_c(Y) \approx (I_p - I_u)\frac{n-k}{nk} + I_u$$

   We invert the previous formula. We obtain

$$k \approx \frac{1}{\frac{I_c(Y) - I_u}{I_p - I_u} + \frac{1}{n}}$$

Solution 2 Vernam with Two Dice

1. In the generalized Vernam cipher, k must be uniformly distributed in $\mathbf{Z}_{12}$. Here, k is a number from 2 to 12. It is not a big deal as it is equivalent to use $k \bmod 12$, but the distribution of $k \bmod 12$ we obtain is far from being uniform in $\mathbf{Z}_{12}$. For instance, $\Pr[k \bmod 12 = 2] = \frac{1}{36}$ and $\Pr[k \bmod 12 = 7] = \frac{1}{6}$.

2. We just have to say for which n is $k \bmod n$ uniformly distributed. Since $k = k_1 + k_2$, the sum of the values k_1 and k_2 of the two dice, and since k_1 and k_2 are independent and uniformly distributed modulo 6, the scheme is secure when n is a factor of 6: $n \in \{1, 2, 3, 6\}$. For $n = 12$, we have seen it is not secure. What remains is $n = 4$.

   $k_1 \bmod 4$ and $k_2 \bmod 4$ have distribution $\Pr[k_i \bmod 4 = i] = \frac{1}{6}$ for $i \in \{0, 3\}$ and $\Pr[k_i \bmod 4 = i] = \frac{1}{3}$ for $i \in \{1, 2\}$. So, $\Pr[k \bmod 4 = 0] = \frac{1}{4}$, $\Pr[k \bmod 4 = 1] = \frac{2}{9}$, $\Pr[k \bmod 4 = 2] = \frac{1}{4}$, and $\Pr[k \bmod 4 = 3] = \frac{5}{18}$. So, it is not uniform and the scheme is not secure for $n = 4$.

3. Using the Bayes formula, we have

$$\Pr[x = b | y = c] = \frac{\Pr[y = c | x = b] \Pr[x = b]}{\sum_{b'} \Pr[y = c | x = b'] \Pr[x = b']}$$

   Clearly, $\Pr[y = c | x = b'] = \Pr[k \equiv c - b' \pmod 4]$ due to the independence between x and k. Since x is uniformly distributed, we obtain

$$\Pr[x = b | y = c] = \frac{\Pr[k \equiv c - b]}{\sum_{b'} \Pr[k \equiv c - b']} = \frac{\Pr[k \equiv c - b]}{\Pr[k \in \{c, c-1\}]}$$

   where values of k are taken modulo 4. Using the distribution that we computed in the previous question, we can fill the following table:

c	$\Pr[x = 0 \mid y = c]$	$\Pr[x = 1 \mid y = c]$
0	9/19	10/19
1	8/17	9/17
2	9/17	8/17
3	10/19	9/19

4. We have $\tilde{x} = 1$ for $c = 0$, $\tilde{x} = 1$ for $c = 1$, $\tilde{x} = 0$ for $c = 2$, and $\tilde{x} = 0$ for $c = 3$. For $x = 0$, $x \neq \tilde{x}$ when $c \in \{0, 1\}$ so $k \bmod 4 \in \{0, 1\}$. For $x = 1$, $x \neq \tilde{x}$ when $c \in \{2, 3\}$ so $k \bmod 4 \in \{1, 2\}$. So, $P_e = \frac{1}{2}\left(\frac{1}{4} + \frac{2}{9}\right) + \frac{1}{2}\left(\frac{2}{9} + \frac{1}{4}\right) = \frac{17}{36} = \frac{1}{2} - \frac{1}{36}$.