Cryptology: Problem Sheet 1

Nilanjan Datta

IAI, TCG CREST

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

2. Prove that, by redefining the key space, we may assume that Enc is deterministic without changing $\mathsf{Pr}[C = c|M = m]$ for any m, c.

3. 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

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

4. Consider an encryption scheme with the message space

$$\mathcal{M} = \{m \in \{0,1\}^{\ell} | \text{ the last bit of m is } 0\}.$$

   Gen chooses a uniform key from $\{0,1\}^{\ell-1}$. $\mathsf{Enc}_k(m)$ returns ciphertext $m \oplus (k\|0)$, and $\mathsf{Dec}_k(c)$ returns $c \oplus (k\|0)$. State and explain whether the above scheme is perfectly secret.

5. Let Π denote the 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) Define $\mathcal{A}$ as follows: $\mathcal{A}$ outputs $m_0 = aab$ and $m_1 = abb$. When given a ciphertext c, it outputs 0 if the first character of c is the same as the second character of c, and outputs 1 otherwise. Compute $\mathsf{Pr}[\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1]$.

   (b) Construct and analyze an adversary $\mathcal{A}'$ for which $\mathsf{Pr}[\mathsf{PrivK}^{eav}_{\mathcal{A},\Pi} = 1]$ is greater than your answer from part (a).