Introduction to Cryptography 20580
Solution to Maman 11

Yehuda Lindell

November 14, 2007

Solution 1: *No solution given.*

Solution 2: Starting with the shift cipher, it suffices to look at the first character in the plaintext and ciphertext; the difference between them is the key. Regarding the substitution cipher, looking at a plaintext character and its corresponding ciphertext character gives the mapping needed. In order to obtain the full key, one needs to look at all (but one) of the English letters in the plaintext. The affine cipher is also easy because given the plaintext and ciphertext we obtain two linear equations in two unknowns which can be solved. Finally, Vigenere's cipher can be broken by finding the different mappings of each plaintext character to a ciphertext character; the period can be computed as in Kasiski's attack (but here it is much easier – I'll leave this to you to see why.) Finally, looking at a plaintext/ciphertext pair in a permutation cipher, the mapping of every unique character is immediate. That is, if in a message of size m the character "a" appears only once then you get the mapping of its position. Specifically, let the unique character be in position i in the plaintext and position j in the ciphertext. Then, it is immediate that $\pi(i) = j$. Regarding non-unique characters, a set of possibilities is obtained. By looking at a few blocks, these possibilities can be reduced and the key derived.

Solution 3:

1. In order to decrypt, take the ith character c'_i and compute $c_i = c'_i - i$. Then, decrypt as for the original cipher.

2. The attack on the substitution cipher does not work in exactly the same way because adding i each time smooths out the statistics. In particular, the plaintext character a is not always mapped to the same ciphertext character (and likewise for all plaintext characters).

3. This question has a surprisingly simple answer. All you need to do is take the ciphertext $c'_1, c'_2, \ldots$ and for every i compute $c_i = c'_i - i$. Then apply the original attack to $c_1, c_2, \ldots$

Solution 4: This modification makes the one-time pad no longer perfectly secret. In order to see this note that after this modification, for every x it holds that $\Pr[x \mid x] = 0$. Therefore, for every x for which $\Pr[x] > 0$ it holds that $\Pr[x \mid x] \neq \Pr[x]$, implying that the scheme is not perfectly secret. The reason why it doesn't matter that the plaintext may be sent unchanged when the key is all zeroes is because the attacker cannot know if the key is all zeroes or something else. Thus it has no way of knowing if the plaintext was unmodified or not.

Solution 5: Assume that $|\mathcal{K}| = |\mathcal{P}| = |\mathcal{C}|$, that every key is obtained with probability $1/|\mathcal{K}|$ and that for every x and y there exists a unique key K such that $e_K(x) = y$. Now, for every $y \in \mathcal{C}$ we have

$$\begin{aligned}\Pr[\mathbf{y} = y] &= \sum_{k \in \mathcal{K}} \Pr[\mathbf{K} = K] \cdot \Pr[\mathbf{x} = d_K(y)] \\ &= \frac{1}{|\mathcal{K}|} \cdot \sum_{k \in \mathcal{K}} \Pr[\mathbf{x} = d_K(y)]\end{aligned}$$

where the first equality is from page 49 of the course book, and the second equality is due to the fact that each key is obtained with probability $1/|\mathcal{K}|$. Next, since for every x and y there exists a unique k such that $e_K(x) = y$ it follows that

$$\sum_{k \in \mathcal{K}} \Pr[\mathbf{x} = d_K(y)] = \sum_{x \in \mathcal{P}} \Pr[\mathbf{x} = x] = 1$$

We conclude that $\Pr[\mathbf{y} = y] = 1/|\mathcal{K}|$. In addition, if $y = e_K(x)$ then $\Pr[\mathbf{y} = y \mid \mathbf{x} = x] = \Pr[\mathcal{K} = K] = 1/|\mathcal{K}|$. We therefore conclude that

$$\Pr[\mathbf{y} = y \mid \mathbf{x} = x] = 1/|\mathcal{K}| = \Pr[\mathbf{y} = y]$$

Applying Bayes' theorem, we have that

$$\Pr[\mathbf{y} = y \mid \mathbf{x} = x] = \frac{\Pr[\mathbf{y} = y]\Pr[\mathbf{x} = x \mid \mathbf{y} = y]}{\Pr[\mathbf{x} = x]}$$

and so

$$\Pr[\mathbf{x} = x \mid \mathbf{y} = y] = \frac{\Pr[\mathbf{y} = y \mid \mathbf{x} = x]\Pr[\mathbf{x} = x]}{\Pr[\mathbf{y} = y]} = \Pr[\mathbf{x} = x]$$

where the second equality is by what we proved above that $\Pr[\mathbf{y} = y \mid \mathbf{x} = x] = \Pr[\mathbf{y} = y]$. We conclude that the scheme achieves perfect secrecy.