HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2024

09/09/2024. Homework for Lecture 1.

Exercise 1. We let $\mathcal{M} = \mathcal{E} = \{A, B, C, \ldots, Z, ' '\}$ (the whole plaintext is a single letter of the latin alphabet or the symbol "blank"), and $\mathcal{K} = \{0, 1, \ldots, 26\}$. We define a cryptographic scheme $\langle \mathtt{Gen}_1, \mathtt{Enc}_1, \mathtt{Dec}_1 \rangle$ as follows:

- $\mathtt{Gen}_1()$ samples a random element of $\mathcal{K}$ with the uniform distribution (every integer $k = 0, 1, \ldots, 26$ is produced with probability $1/27$).
- The encoding $\mathtt{Enc}_1(m, k)$ maps each letter m of the latin alphabet to the letter which stands in the alphabet k positions later (modulo 27) than m. For example, $\mathtt{Enc}_1(A, 3) = D$, $\mathtt{Enc}_1(F, 5) = K$, $\mathtt{Enc}_1(X, 3) = ' '$, $\mathtt{Enc}_1(Y, 4) = B$.
- The decoding $\mathtt{Dec}_1(e, k)$ maps each letter e of the latin alphabet to the letter which appears in the alphabet k positions earlier (again, modulo 27) than e. For example, $\mathtt{Dec}_1(A, 3) = Y$, $\mathtt{Dec}_1(F, 5) = A$, $\mathtt{Dec}_1(Y, 4) = U$.

Prove that this scheme satisfies the definition of a secure encryption scheme.

Hint: Adapt to this case the argument from Theorem 2 discussed in the class.

Exercise 2. We let $\mathcal{M} = \mathcal{E} = \{A, B, C, \ldots, Z, ' '\}^{100}$ (the plaintext is a sequence of 100 symbols where each symbol is either a letter of the latin alphabet or the symbol "blank"), and $\mathcal{K} = \{0, 1, \ldots, 26\}^{100}$. We define a cryptographic scheme $\langle \mathtt{Gen}_2, \mathtt{Enc}_2, \mathtt{Dec}_2 \rangle$ as follows:

- $\mathtt{Gen}_2()$ samples a random element of $(k^1 \ldots k^{100}) \in \{0, 1, \ldots, 26\}^{100}$ with the uniform distribution.
- The encoding $\mathtt{Enc}_2$ is a letter-wise repetition of $\mathtt{Enc}_1$ from Exercise 1: for each $(m^1 \ldots m^{100}) \in \mathcal{M}$ and each $(k^1 \ldots k^{100}) \in \mathcal{K}$

  $$\mathtt{Enc}_2((m^1 \ldots m^{100}), (k^1 \ldots k^{100})) := (\mathtt{Enc}_1(m^1, k^1)\, \mathtt{Enc}_1(m_2, k^2)\ \ldots\ \mathtt{Enc}_1(m^{100}, k^{100})),$$

  i.e., we "shift" each letter m_i by k_i steps to the right in the alphabet (modulo 27).

Prove that this scheme satisfies the definition of a secure encryption scheme.

Exercise 3 (optional)**.** The *substitution encryption scheme* with some unknown permutation

$$\pi\ :\ \{A, B, C, \ldots, Z, ' '\} \to \{A, B, C, \ldots, Z, ' '\}$$

was used to encode a french text (with omitted apostrophes and punctuation marks, with no accents and no capital letters). The encoded text is

```
nbxcubftvbygmbgvlvxbxubfgevbhxbarxmblxbhbxutubkexbhxbf
gvuxevblebfvxcxmubtbztrubnxbkebrhbtbztrubuvgrcblxnxyav
xbyrhhxbcrjbnxmubormsubcrjbqxbogecbfvrxblbtsvxxvbbytlt
yxbygmcrxevbhbxjfvxccrgmblxbyxcbctheuturgmcblrcurmsexx
cbvrnwxhrxeb
```

Reconstruct the clear text.

Hint: Use the fact that different letters and combinations of letters have different frequencies in the French language.