Solutions to Problem Set 2

Problem 2: Affine Cipher (2.13.4)

From the chosen plaintext attack, we have

$$\begin{cases} 0\alpha + \beta \equiv 14 \pmod{26} \\ 7\alpha + \beta \equiv 13 \pmod{26} \end{cases}$$

We get $\beta \equiv 14 \pmod{26}$ immediately, and then obtain $7\alpha \equiv -1 \pmod{26}$. Using Extended Euclidean Algorithm, we can easily get $7^{-1} \equiv -11 \pmod{26}$, so $\alpha \equiv 11 \pmod{26}$. Thus, the decryption function is $x \mapsto 11x + 14 \pmod{26}$.

Problem 3: Vigenere Cipher (2.13.10)

You can make left shifting or right shifting or left wrapping shifting or right wrapping shifting to calculate the number of coincidences and come to the result that the key length is probably 2.

From the letter frequency, we have $A_0 = \{0.1, 0.9\}$. We study the odd positions of the ciphertext and get $W = \{0.2, 0.8\}$. Obviously, $W \cdot A_0 > W \cdot A_1$, so the first key is $0 = a$. Similarly, we obtain the second key is $1 = b$. And finally we decrypt the ciphertext to get *bbbbbbabbb*.

Problem 4: Hill Cipher (2.13.15)

From the chosen plaintext attack, we have

$$\begin{pmatrix} 1 & 0 \\ 25 & 25 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 7 & 2 \\ 6 & 19 \end{pmatrix} \pmod{26}.$$

Since

$$\det \begin{pmatrix} 1 & 0 \\ 25 & 25 \end{pmatrix} \equiv 25 \equiv -1 \pmod{26},$$

and $\gcd(-1, 26) = 1$, we have $(-1)^{-1} \equiv -1 \pmod{26}$. So we obtain the inverse matrix

$$\begin{pmatrix} 1 & 0 \\ 25 & 25 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}.$$

Thus

$$M \equiv \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 7 & 2 \\ 6 & 19 \end{pmatrix} \equiv \begin{pmatrix} 7 & 2 \\ -13 & -21 \end{pmatrix} \equiv \begin{pmatrix} 7 & 2 \\ 13 & 5 \end{pmatrix} \pmod{26}.$$

Problem 5: LFSR Machine (2.13.21)

Pick the sequences with 0 to make the answer evident.

$$\begin{cases} c_0 x_2 + c_1 x_3 \equiv x_4 \pmod{3} \\ c_0 x_6 + c_1 x_7 \equiv x_8 \pmod{3} \end{cases}$$

We immediately get $c_0 \equiv 2 \pmod{3}$ and $c_1 \equiv 1 \pmod{3}$.

Problem 6: Chaining Modes

ECB : All other ciphertext blocks except the lost one can be decrypted correctly.

CBC : The lost ciphertext block and the sequential one can't be correctly decrypted, while all other blocks can be.

CFB : The lost ciphertext block and the sequential one can't be correctly decrypted, while all other blocks can be.

OFB : All other ciphertext blocks except the lost one can be decrypted correctly.

PCBC : The lost ciphertext block and all the sequential ones can't be correctly decrypted.

Problem 7: Birthday Paradox Calculation

Since $p_m = 1 - \text{prob}[\text{two subsets have an empty intersection}]$, we compute the item on the right side first. There are totally $\binom{100}{m}\binom{100}{m}$ choices to draw two random subsets of size m, and there are $\binom{100}{m}\binom{100-m}{m}$ choices to draw two non-overlapped random subsets of the same size. We obtain that

$$p_m = 1 - \frac{\binom{100}{m}\binom{100-m}{m}}{\binom{100}{m}\binom{100}{m}} = 1 - \sum_{i=0}^{m-1} \frac{100-m-i}{100-i}.$$

Use a program to try $m = 1 \cdots 20$, and get $m = 9$ for $p_m \geq 1/2$ and $m = 12$ for $p_m \geq 3/4$.

Problem 8: Meet-in-the-Middle Attack

(a) We are guaranteed of finding at least one match, since if (k_1, k_2) is the real key pair used in the double encryption, then $E_{k_1}(m) = D_{k_2}(c)$.

(b) If there is only one match, then we have found the key pair and broken the system. If there are several matches, we know that the key pair is one of the matching pairs. This set is likely to be much much smaller than the original key space, so they can each be tried on additional plaintext-ciphertext pairs to find which ones work.

(c) Considering a double Caesar cipher, no matter what keys you are choosing, X_m and X_c will generate the all 26 letters of the whole space. So $X_m \bigcap X_c = 26 \geq 2$.