YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467a: Cryptography and Computer Security *Handout #9*

Felipe Saint-Jean *October 9, 2005*

Solutions to Problem Set 1

Problem 1 (2.13.2)

First notice that $9 \cdot 3 \equiv_{26} 1$. That means that 9 and 3 are inverses in $\pmod{26}$. Given that and the encryption function, $E(x) = 9x + 2$, the decryption function is $D(x) = 3x - 6$. So

$$D(U = 20) = 3 \cdot 20 - 6 = 54 \equiv_{26} 2 = C$$

$$D(C = 2) = 3 \cdot 2 - 6 \equiv_{26} 0 = A$$

$$D(R = 17) = 3 \cdot 17 - 6 \equiv_{26} 19 = T$$

Problem 2 (2.13.11)

Let's first notice that if the key is of length k then the m-th letter of the plain-text, P_m, was encrypted with the $m \bmod k$ letter of the key $K_{m \bmod k}$. That means that given the key length we can separate the cipher-text in subsets of letters that were encrypted with the same key, therefore a frequency analysis will get some information on each subset them.

The cyphertext, written numerically, is 0121011102.

For key size one we do a simple count

position	0	1	2
0	0.3	0.5	0.2

For key size of two we will distinguish keys in position $\equiv_2 0$ and $\equiv_2 1$ in the text

position	0	1	2
0	0.3	0.1	0.1
1	0	0.4	0.1

Notice that if we shift row 1 one to the left and add up the columns we get the exact distribution given distribution. So size two is a good candidate.

For key size three similar thing but we have to consider 3 possible positions for each letter.

position	0	1	2
0	0.083	0.16	0.083
1	0.111	0.222	0
2	0.111	0.111	0.111

In this case is clear that no matter how we shift the rows we don't get to a distribution close to the objective. The best candidate is $k = 2$ for shift 0 $a \to a$ and for shift 1 $a \to b$ so the most likely key is ab.

Problem 3 (2.13.13)

The Hill cipher of size 2 takes pairs of letters and encrypts them by multiplying them by a key matrix. To decrypt it we need to invert the matrix using modular arithmetic:

$$\begin{pmatrix} 9 & 13 \\ 2 & 3 \end{pmatrix}^{-1} = \frac{1}{9 \cdot 3 - 2 \cdot 13} \begin{pmatrix} 3 & -13 \\ -2 & 9 \end{pmatrix}$$

So far we have only used the standard 2×2 matrix inversion formula. Now we need to do all the operations $\bmod 26$. So $9 \cdot 3 - 2 \cdot 13 \equiv_{26} 1$, $-2 \equiv_{26} 26 - 2 \equiv_{26} 24$, $-13 \equiv_{26} 26 - 13 \equiv_{26} 13$. Then the inverse is

$$\begin{pmatrix} 3 & 13 \\ 24 & 9 \end{pmatrix}$$

Since $C = P \cdot A$ then $P = C \cdot A^{-1}$ so

$$\begin{aligned} \begin{pmatrix} P_1 & P_2 \end{pmatrix} &= \begin{pmatrix} Y = 24 & I = 8 \end{pmatrix} \cdot \begin{pmatrix} 3 & 13 \\ 24 & 9 \end{pmatrix} \\ &= \begin{pmatrix} 3 \cdot 24 + 8 \cdot 24 & 13 \cdot 24 + 9 \cdot 8 \end{pmatrix} \equiv_{26} \begin{pmatrix} 4 = e & 20 = u \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \begin{pmatrix} P_3 & P_4 \end{pmatrix} &= \begin{pmatrix} F = 5 & Z = 25 \end{pmatrix} \cdot \begin{pmatrix} 3 & 13 \\ 24 & 9 \end{pmatrix} \\ &= \begin{pmatrix} 3 \cdot 5 + 25 \cdot 24 & 13 \cdot 5 + 9 \cdot 25 \end{pmatrix} \equiv_{26} \begin{pmatrix} 17 = r & 4 = e \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \begin{pmatrix} P_5 & P_6 \end{pmatrix} &= \begin{pmatrix} M = 12 & A = 0 \end{pmatrix} \cdot \begin{pmatrix} 3 & 13 \\ 24 & 9 \end{pmatrix} \\ &= \begin{pmatrix} 12 \cdot 3 + 0 \cdot 24 & 13 \cdot 12 + 0 \cdot 9 \end{pmatrix} \equiv_{26} \begin{pmatrix} 10 = k & 0 = a \end{pmatrix} \end{aligned}$$

Problem 4 (2.13.20)

A sequence generated by the given recurrence would look like $10101010101010101\ldots$. If we assume that $x_{n+2} = c_0 \cdot x_n + c_1 \cdot x_{n+1}$ we can write the equations for a recurrence of size 2 for the first 4 values of the series:

$$1 \equiv c_0 \cdot 1 + c_1 \cdot 0$$

$$0 \equiv c_0 \cdot 0 + c_1 \cdot 1$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$$

Solving for the system we get that $c_0 = 1$ and $c_1 = 0$. Therefore the recurrence is $x_{n+2} = 0 \cdot x_n + 1 \cdot x_{n+1}$.

Problem 5 (2.13.23)

$\frac{10^{100}}{120 \cdot 365 \cdot 24 \cdot 60 \cdot 60} \approx 2 \cdot 10^{90} \ldots$ a lot if you think that a modern computer runs at around 4 Ghz that can count at most $4 \cdot 10^9$ numbers per second.

Problem 6 (15.6.9)

a

$$H(P) = -\sum p_i \log p_i = -\frac{1}{3} \log \frac{1}{3} - \frac{2}{3} \log \frac{2}{3}$$

b

If we redefine $a = 0$, $A = 0$, $b = 1$, $B = 1$, $k_1 = 0$ and $k_2 = 1$ the mentioned cipher is one time pad, so it has perfect secrecy. Then

$$H(P|C) = H(P)$$