

Cryptography Assignment 2 was marked out of 40 and contributes 5% towards your final mark.

1. (a) (6 marks)

$$p_C(A) = p_{\mathcal{P}}(a)p_{\mathcal{K}}(K_1) + p_{\mathcal{P}}(c)p_{\mathcal{K}}(K_2) + p_{\mathcal{P}}(b)p_{\mathcal{K}}(K_3) = \left(\frac{3}{8}\right) \left(\frac{1}{3}\right) + \left(\frac{1}{2}\right) \left(\frac{1}{2}\right) + \left(\frac{1}{8}\right) \left(\frac{1}{6}\right) = \frac{19}{48}$$

$$p_C(B) = p_{\mathcal{P}}(b)p_{\mathcal{K}}(K_1) + p_{\mathcal{P}}(a)p_{\mathcal{K}}(K_2) + p_{\mathcal{P}}(c)p_{\mathcal{K}}(K_3) = \left(\frac{1}{8}\right) \left(\frac{1}{3}\right) + \left(\frac{3}{8}\right) \left(\frac{1}{2}\right) + \left(\frac{1}{2}\right) \left(\frac{1}{6}\right) = \frac{5}{16}$$

$$p_C(C) = p_{\mathcal{P}}(c)p_{\mathcal{K}}(K_1) + p_{\mathcal{P}}(b)p_{\mathcal{K}}(K_2) + p_{\mathcal{P}}(a)p_{\mathcal{K}}(K_3) = \left(\frac{1}{2}\right) \left(\frac{1}{3}\right) + \left(\frac{1}{8}\right) \left(\frac{1}{2}\right) + \left(\frac{3}{8}\right) \left(\frac{1}{6}\right) = \frac{7}{24}$$

(b) (2 marks) Since $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$ Shannon's Theorem says that this cryptosystem does not have perfect secrecy since the keys are not used with equal probability.

(Alternatively, you could have shown that $p_{\mathcal{P}}(x|y) \neq p_{\mathcal{P}}(x)$ for some $x \in \{a, b, c\}$ and some $y \in \{A, B, C\}$.)

2. (8 marks) First note that the subkeys are $k_1 = (124)(3)$, $k_2 = (142)(3)$ and $k_3 = (1)(2)(3)(4)$. Since the ciphertext is written by reversing the two halves, $L_3 = 1110$ and $R_3 = 1001$. Thus

$$R_2 = L_3 = 1110 \quad \text{and} \quad L_2 = R_3 \oplus f(R_2, k_3) = 1001 \oplus 1110 = 0111.$$

Next

$$R_1 = L_2 = 0111 \quad \text{and} \quad L_1 = R_2 \oplus f(R_1, k_2) = 1110 \oplus 1011 = 0101.$$

Finally

$$R_0 = L_1 = 0101 \quad \text{and} \quad L_0 = R_1 \oplus f(R_0, k_1) = 0111 \oplus 1100 = 1011$$

Thus the plaintext was 10110101.

3. (6 marks) The (hex) key 1FE01FE00EF10EF1 corresponds to the binary key

$$K = 0001\ 1111\ 1110\ 0000\ 0001\ 1111\ 1110\ 0000\ 0000\ 1110\ 1111\ 0001\ 0000\ 1110\ 1111\ 0001$$

Thus $PC_1(K) = C_0D_0$ where

$$C_0 = 1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010\ 1010 \quad \text{and} \quad D_0 = 0101\ 0101\ 0101\ 0101\ 0101\ 0101\ 0101\ 0101.$$

A shift of C_0 by one or two positions gives either 1010... or 0101... and the corresponding shift of D_0 gives either 0101... or 1010.... Thus, there are only two possibilities for C_iD_i :
1010 1010 1010 1010 1010 1010 1010 0101 0101 0101 0101 0101 0101 0101 0101
or 0101 0101 0101 0101 0101 0101 0101 1010 1010 1010 1010 1010 1010 1010.

Hence there are only two subkeys generated by the key schedule so this is a semi-weak key and is not a good choice for use in DES. The two subkeys are:

$$0110\ 1110\ 1010\ 1100\ 0001\ 1010\ 0100\ 0011\ 0001\ 1001\ 1011\ 1101$$

$$1001\ 0001\ 0101\ 0011\ 1110\ 0101\ 1011\ 1100\ 1110\ 0110\ 0100\ 0010$$

Please turn over.

4. (a) (2 marks) $\{42\}$ can be written as the bitstring $\{01000010\}$ and the polynomial $x^6 + x$. $\{a3\}$ can be written as the bitstring $\{10100011\}$ and the polynomial $x^7 + x^5 + x + 1$.
- (b) (2 marks) $\{42\} \oplus \{a3\} = x^7 + x^6 + x^5 + 1 = 11100001 = \{e1\}$.
- (c) (2 marks) We are multiplying modulo $m(x) = x^8 + x^4 + x^3 + x + 1$. You can do this by multiplying to find a polynomial $p(x)$ and then doing long division to find the remainder $r(x)$ where $p(x) = q(x)m(x) + r(x)$ and $\text{degree } r(x) < 8$, or you can use the short-cut of replacing every occurrence of x^8 in $p(x)$ by $x^8 = x^4 + x^3 + x + 1$.

$$\begin{aligned}
 \{42\} \cdot \{a3\} &= (x^6 + x)(x^7 + x^5 + x + 1) \\
 &= x^{13} + x^{11} + x^8 + x^7 + x^6 + x^6 + x^2 + x \\
 &= x^5(x^4 + x^3 + x + 1) + x^3(x^4 + x^3 + x + 1) + (x^4 + x^3 + x + 1) + x^7 + x^2 + x \\
 &= x^9 + x^8 + x^6 + x^5 + x^7 + x^6 + x^4 + x^3 + x^4 + x^3 + x + 1 + x^7 + x^2 + x \\
 &= x(x^4 + x^3 + x + 1) + (x^4 + x^3 + x + 1) + x^5 + 1 + x^2 \\
 &= x^5 + x^4 + x^2 + x + x^4 + x^3 + x + 1 + x^5 + 1 + x^2 \\
 &= x^3
 \end{aligned}$$

- (d) (2 marks) By Table 2 $\{42\} = \{03\}^{\{db\}}$ and $\{a3\} = \{03\}^{\{6f\}}$. But converting to decimals gives $\{db\} + \{6f\} = 219 + 111 = 330$ and $330 - 255 = 75$ which is $\{4b\}$ in hex. Thus

$$\{42\} \cdot \{a3\} = \{03\}^{\{db\}} \cdot \{03\}^{\{6f\}} = \{03\}^{\{4b\}} = \{08\}$$

by Table 3. This is in agreement with the result of part (c).

- (e) (2 marks) By Table 2 $\{42\} = \{03\}^{\{db\}}$. Thus the inverse of $\{42\}$ is

$$\{03\}^{\{ff\} - \{db\}} = \{03\}^{\{24\}} = \{37\}$$

by Table 3. Notice that you can check this by multiplying the polynomials $x^6 + x$ and $x^5 + x^4 + x^2 + x + 1$ to give 1.

5. (8 marks) Attached to this document are two pages of answers related to RSA. The second page is for the Chinese Remainder Theorem calculation (part (c)).