

These questions are based on the material in Section 4: Shannon’s Theory, Section 5: Modern Cryptography, Section 6: The Data Encryption Standard, Section 7: International Data Encryption Algorithm, Section 9: AES Technical Detail and Section 10: Public Key Cryptography: RSA. You do not need to submit your answers to any of these questions.

1. Let $\mathcal{P} = \{0, 1, 2\}$ with $p_{\mathcal{P}}(0) = 1/3$, $p_{\mathcal{P}}(1) = 1/4$ and $p_{\mathcal{P}}(2) = 5/12$.
 Let $\mathcal{K} = \{k_1, k_2, k_3, k_4\}$ with $p_{\mathcal{K}}(k_i) = 1/4$ for $i = 1, 2, 3, 4$. Let $\mathcal{C} = \{0, 1, 2\}$.
 Define $e_{k_i}(x) = 2x + i \pmod{3}$, for $x \in \{0, 1, 2\}$ and $i \in \{1, 2, 3, 4\}$.
 - (a) Determine $p_{\mathcal{C}}(y)$ for $y = 0, 1, 2$.
 - (b) Determine $p_{\mathcal{P}}(0|1)$ and $p_{\mathcal{P}}(1|2)$.
 - (c) Give an example to show that this cryptosystem does not have perfect secrecy.
2. Suppose that the 312 keys of the affine cipher are used with equal probability $1/312$. Prove that for any plaintext distribution of the 26 letter plaintext alphabet, the affine cipher has perfect secrecy.
3. Consider a 3-stage Feistel cipher defined with a function f as $f((x_1, x_2, x_3, x_4, x_5), \pi) = (x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, x_{\pi(4)}, x_{\pi(5)})$. Let the initial key be the permutation $(135)(24)$ and let each subkey k_i be the permutation obtained by applying the initial key permutation i times. Determine the ciphertext for the plaintext 0010111001.
4. Applying the first stage of a Feistel cipher with first subkey $k_1 = (123)$ and function $f((x_1, x_2, x_3), \pi) = (x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)})$ resulted in $L_1R_1 = 010110$. Determine the corresponding plaintext.
5. Using the (hexadecimal) key 010145458989C D C D, the first subkey for DES is

$$K_1 = 0000\ 1011\ 0000\ 0010\ 0100\ 0011\ 1001\ 1001\ 0100\ 1000\ 0010\ 0100.$$

Perform the first round of DES encryption on the (hexadecimal) plaintext

$$02468ACE13579BDF$$

using this key.

6. Determine the decryption keys for the first round of IDEA decryption using the (hexadecimal) key 00112233445566778899aabbccddeeff.

7. Using the notation from the AES specification paper, determine the following.
- (a) Determine the bitstring representations and the polynomial representations of the 2-digit hex field elements $\{7f\}$ and $\{4e\}$.
 - (b) Determine $\{7f\} \oplus \{4e\}$.
 - (c) Determine $\{7f\} \cdot \{4e\}$ using polynomial multiplication.
 - (d) Verify your answer from (c) by finding $\{7f\} \cdot \{4e\}$ using Tables 2 and 3 from the AES specification paper.
 - (e) Determine the multiplicative inverse of the field element $\{4e\}$.
8. Use the properties listed in Remark 10.7 of the notes to prove that if p is a prime number and n is a positive integer, then

$$\phi(pn) = \begin{cases} (p-1)\phi(n) & \text{if } p \text{ does not divide } n \\ p\phi(n) & \text{if } p \text{ does divide } n \end{cases}$$

9. Suppose that Bob has set up an RSA scheme with $p = 191$, $q = 127$ and $b = 47$.
- (a) Compute n , $\phi(n)$ and a .
 - (b) Alice looks up the public key (b, n) and uses these to encrypt the message 2468. What is the encrypted message that she sends to Bob?
 - (c) Alice later sends another message to Bob, this time the message is 9625. Use the Chinese Remainder Theorem (as in Algorithm 10.20 from the notes) to decrypt the message.

1. (a)

$$\begin{aligned} p_{(C)}(0) &= p_{\mathcal{K}}(k_1)p_{\mathcal{P}}(1) + p_{\mathcal{K}}(k_2)p_{\mathcal{P}}(2) + p_{\mathcal{K}}(k_3)p_{\mathcal{P}}(0) + p_{\mathcal{K}}(k_4)p_{\mathcal{P}}(1) \\ &= \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) \\ &= \frac{5}{16} \end{aligned}$$

$$\begin{aligned} p_{(C)}(1) &= p_{\mathcal{K}}(k_1)p_{\mathcal{P}}(0) + p_{\mathcal{K}}(k_2)p_{\mathcal{P}}(1) + p_{\mathcal{K}}(k_3)p_{\mathcal{P}}(2) + p_{\mathcal{K}}(k_4)p_{\mathcal{P}}(0) \\ &= \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) \\ &= \frac{1}{3} \end{aligned}$$

$$\begin{aligned} p_{(C)}(2) &= p_{\mathcal{K}}(k_1)p_{\mathcal{P}}(2) + p_{\mathcal{K}}(k_2)p_{\mathcal{P}}(0) + p_{\mathcal{K}}(k_3)p_{\mathcal{P}}(1) + p_{\mathcal{K}}(k_4)p_{\mathcal{P}}(2) \\ &= \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{5}{12}\right) \\ &= \frac{17}{48} \end{aligned}$$

$$(b) \quad p_{\mathcal{P}}(0|1) = \frac{p_{\mathcal{P}}(0)p_{(C)}(1|0)}{p_{(C)}(1)} = \frac{1/3(1/4 + 1/4)}{1/3} = \frac{1}{2}$$

$$p_{\mathcal{P}}(1|2) = \frac{p_{\mathcal{P}}(1)p_{(C)}(2|1)}{p_{(C)}(2)} = \frac{1/4(1/4)}{17/48} = \frac{3}{17}$$

(c) Since $p_{\mathcal{P}}(0|1) = \frac{1}{2} \neq p_{\mathcal{P}}(0) = \frac{1}{3}$, this system does not have perfect secrecy.

2. Suppose that the 312 keys of the affine cipher are used with equal probability $1/312$ so for each $k \in \mathcal{K}$ we have $p_{\mathcal{K}}(k) = \frac{1}{312}$. Since $26 = |\mathcal{P}| \neq |\mathcal{K}| = 312$ we cannot use Shannon's Theorem.

We first need to show that for each pair of plaintext-ciphertext letters (x, y) , there are exactly 12 keys that encrypt x to y . For each choice of a , the key $(a, y - ax)$ encrypts the plaintext letter x to the ciphertext letter y , since $ax + (y - ax) = y$. There are twelve possible choices for a so there are exactly twelve keys that map a given plaintext letter to a given ciphertext letter. Thus

$$p_{(C)}(y) = \sum_{k \in \mathcal{K}} p_{\mathcal{K}}(k)p_{\mathcal{P}}(d_k(y)) = \frac{12}{312}p_{\mathcal{P}}(a) + \frac{12}{312}p_{\mathcal{P}}(b) + \cdots + \frac{12}{312}p_{\mathcal{P}}(z) = \frac{12}{312} \times 1 = \frac{1}{26}.$$

Also $p_{(C)}(y|x) = \sum_{k: x=d_k(y)} p_{\mathcal{K}}(k) = \frac{12}{312} = \frac{1}{26}$, as each key occurs with probability $\frac{1}{312}$ and there are twelve keys that decrypt x to y , that is twelve keys for which $x = d_k(y)$.

Hence

$$p_{\mathcal{P}}(x|y) = \frac{p_{\mathcal{P}}(x)p_{(C)}(y|x)}{p_{(C)}(y)} = \frac{p_{\mathcal{P}}(x)\frac{1}{26}}{\frac{1}{26}} = p_{\mathcal{P}}(x)$$

and so this cryptosystem has perfect secrecy.

3. $L_0 = 00101$ and $R_0 = 11001$. The subkeys are $k_1 = (135)(24)$, $k_2 = (153)(2)(4)$ and $k_3 = (1)(5)(3)(24)$. Thus we have $L_1 = R_0 = 11001$ and

$$R_1 = L_0 \oplus f(R_0, k_1) = 00101 \oplus 00111 = 00010$$

Next we have $L_2 = R_1 = 00010$ and

$$R_2 = L_1 \oplus f(R_1, k_2) = 11001 \oplus 00010 = 11011$$

Finally we have $L_3 = R_2 = 11011$ and

$$R_3 = L_2 \oplus f(R_2, k_3) = 00010 \oplus 11011 = 11001$$

The ciphertext is $R_3L_3 = 1100111011$.

4. We have $L_1 = 010$ and $R_1 = 110$. From the Feistel equations we get $R_0 = L_1 = 010$ and

$$L_0 = R_1 \oplus f(R_0, k_1) = 110 \oplus 100 = 010.$$

Thus the plaintext was 010010.

5. Converting the plaintext x to binary gives:

hex	0	2	4	6	8	A	C	E
binary	0000	0010	0100	0110	1000	1010	1100	1110
hex	1	3	5	7	9	B	D	F
binary	0001	0011	0101	0111	1001	1011	1101	1111

Then $IP(x) = L_0R_0$ where

$$\begin{aligned} L_0 &= 1010 & 1010 & 1111 & 0000 & 1010 & 1010 & 1111 & 0000 \\ R_0 &= 1100 & 1100 & 0000 & 0000 & 1100 & 1100 & 1111 & 1111 \end{aligned}$$

To apply the Feistel equations we will need to calculate $f(R_0, K_1)$. We do this in stages.

$$E(R_0) = 1110\ 0101\ 1000\ 0000\ 0000\ 0001\ 0110\ 0101\ 1001\ 0111\ 1111\ 1111.$$

Then we XOR $E(R_0)$ with K_1 (given in the question) and write the result in groups of six.

$$E(R_0) \oplus K_1 = 111011\ 101000\ 001001\ 000010\ 111111\ 001101\ 111111\ 011011.$$

For the first S -box, we have row 11, column 1101 which gives 0. For the second S -box we have row 10, column 0100 which gives 10. For the third S -box we have row 01, column 0100 which gives 3. For the fourth S -box we have row 00, column 0001 which gives 13. For the fifth S -box we have row 11, column 1111 which gives 3. For the sixth S -box we have row 01, column 0110 which give 9. For the seventh S -box we have row 11, column 1111 which gives 12. For the eighth S -box we have row 01, column 1101 which gives 14. Thus $C = 0000\ 1010\ 0011\ 1101\ 0011\ 1001\ 1100\ 1110$ so

$$P(C) = f(R_0, K_1) = 1111\ 1100\ 0001\ 1010\ 0011\ 0000\ 1110\ 0101.$$

Hence we have

$$\begin{aligned} L_1 = R_0 &= 1100 & 1100 & 0000 & 0000 & 1100 & 1100 & 1111 & 1111 \\ R_1 = L_0 \oplus f(R_0, K_1) &= 0101 & 0110 & 1110 & 1010 & 1001 & 1010 & 0001 & 0101 \end{aligned}$$

6. As given in the lecture notes $DK_1^{(1)} = (K_1^{(9)})^{-1}$, $DK_2^{(1)} = -(K_2^{(9)})$, $DK_3^{(1)} = -(K_3^{(9)})$, $DK_4^{(1)} = (K_4^{(9)})^{-1}$, $DK_5^{(1)} = K_5^{(8)}$, $DK_6^{(1)} = K_6^{(8)}$

We can use the key generation table from the notes to determine which bits of the key to use for the subkeys needed.

Converting the key to binary gives:

hex	0	0	1	1	2	2	3	3	4	4	5
binary	0000	0000	0001	0001	0010	0010	0011	0011	0100	0100	0101
hex	5	6	6	7	7	8	8	9	9	a	a
binary	0101	0110	0110	0111	0111	1000	1000	1001	1001	1010	1010
hex	b	b	c	c	d	d	e	e	f	f	
binary	1011	1011	1100	1100	1101	1101	1110	1110	1111	1111	

Bits 22 – 37 give $K_1^{(9)} = 0100\ 0110\ 0110\ 1000 = 18024$

Bits 38 – 53 give $K_2^{(9)} = 1000\ 1010\ 1010\ 1100 = 35500$

Bits 54 – 69 give $K_3^{(9)} = 1100\ 1110\ 1111\ 0001 = 52977$

Bits 70 – 85 give $K_4^{(9)} = 0001\ 0011\ 0011\ 0101 = 4917$

Bits 93 – 108 give $K_5^{(8)} = 1011\ 1100\ 1100\ 1101$

Bits 109 – 124 give $K_6^{(8)} = 1101\ 1110\ 1110\ 1111$

$$\begin{aligned} DK_1^{(1)} &= (K_1^{(9)})^{-1} = (18024)^{-1} \bmod 65537 = 45753 \\ &= 1011\ 0010\ 1011\ 1001 \end{aligned}$$

$$\begin{aligned} DK_2^{(1)} &= -(K_2^{(9)}) = -35500 \bmod 65536 = 30036 \\ &= 0111\ 0101\ 0101\ 0100 \end{aligned}$$

$$\begin{aligned} DK_3^{(1)} &= -(K_3^{(9)}) = -52977 \bmod 65536 = 12559 \\ &= 0011\ 0001\ 0000\ 1111 \end{aligned}$$

$$\begin{aligned} DK_4^{(1)} &= (K_4^{(9)})^{-1} = (4917)^{-1} \bmod 65537 = 18047 \\ &= 0100\ 0110\ 0111\ 1111 \end{aligned}$$

$$DK_5^{(1)} = K_5^{(8)} = 1011\ 1100\ 1100\ 1101$$

$$DK_6^{(1)} = K_6^{(8)} = 1101\ 1110\ 1110\ 1111$$

7. (a) $\{7f\} = 01111111 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $\{4e\} = 01001110 = x^6 + x^3 + x^2 + x$

(b) $\{7f\} \oplus \{4e\} = 01111111 \oplus 01001110 = 00110001 = \{31\}$.

(c) $\{7f\} \cdot \{4e\}$

$$\begin{aligned} &= (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x^6 + x^3 + x^2 + x) \\ &= x^{12} + x^9 + x^8 + x^7 + x^{11} + x^8 + x^7 + x^6 + x^{10} + x^7 + x^6 + x^5 + x^9 + \\ &\quad x^6 + x^5 + x^4 + x^8 + x^5 + x^4 + x^3 + x^7 + x^4 + x^3 + x^2 + x^6 + x^3 + x^2 + x \\ &= x^{12} + x^{11} + x^{10} + x^8 + x^5 + x^4 + x^3 + x \\ &= x^4(x^4 + x^3 + x + 1) + x^3(x^4 + x^3 + x + 1) + x^2(x^4 + x^3 + x + 1) + x^4 + \\ &\quad x^3 + x + 1 + x^5 + x^4 + x^3 + x \\ &= x^4 + x^3 + x + 1 + x^7 + x^5 + x^4 + x^7 + x^6 + x^4 + x^3 + x^6 + x^5 + x^3 + x^2 + x^5 + 1 \\ &= x^5 + x^4 + x^3 + x^2 + x \\ &= \{3e\} \end{aligned}$$

(d) Using Tables 2 and 3, we have

$$\{7f\} \cdot \{4e\} = \{03\}^{\{57\}} \cdot \{03\}^{\{83\}} = \{03\}^{\{57\}+\{83\}} = \{03\}^{\{da\}} = \{3e\}.$$

(e) $\{4e\} = \{03\}^{\{83\}}$ so its multiplicative inverse is $\{03\}^{\{ff\}-\{83\}} = \{03\}^{\{7c\}} = \{e9\}$.
You can check this by multiplying the polynomials $x^6 + x^3 + x^2 + x$ and $x^7 + x^6 + x^5 + x^3 + 1$.

8. If p does not divide n , then $\gcd(p, n) = 1$ and properties 1 and 3 of Remark 10.7 tell us that $\phi(pn) = \phi(p)\phi(n) = (p-1)\phi(n)$ as required.

If p does divide n then let $n = p^k m$ where $\gcd(p, m) = 1$ and $k \geq 1$. Then

$$\begin{aligned} \phi(pn) &= \phi(p^{k+1}m) && \text{since } n = p^k m \\ &= \phi(p^{k+1})\phi(m) && \text{by property 3 since } \gcd(p, m) = 1 \\ &= (p^{k+1} - p^k)\phi(m) && \text{by property 2} \end{aligned}$$

Furthermore,

$$p\phi(n) = p\phi(p^k m) = p\phi(p^k)\phi(m) = p(p^k - p^{k-1})\phi(m) = (p^{k+1} - p^k)\phi(m)$$

as required.

9. Here $p = 191$, $q = 127$ and $b = 47$.

(a) We have $n = 191 \times 127 = 24257$ and $\phi(n) = 190 \times 126 = 23940$.
Then $a = 47^{-1} \bmod 23940$ so we apply the Euclidean algorithm.

$$\begin{array}{ll} 23940 &= 509(47) + 17 & 1 &= 13 - 3(4) \\ 47 &= 2(17) + 13 & &= 13 - 3(17 - 13) \\ 17 &= 13 + 4 & &= 4(13) - 3(17) \\ 13 &= 3(4) + 1 & &= 4(47 - 2(17)) - 3(17) \\ & & &= 4(47) - 11(17) \\ & & &= 4(47) - 11(23940 - 509(47)) \\ & & &= 5603(47) - 11(23940) \end{array}$$

Thus $a = 5603$.

(b) Alice must send the message $2468^{47} \bmod 24257$. To calculate this we use the fact that $47 = 32 + 8 + 4 + 2 + 1$.

$$\begin{aligned} (2468)^2 &= 2517 \bmod 24257 \\ (2468)^4 &= (2517)^2 = 4212 \bmod 24257 \\ (2468)^8 &= (4212)^2 = 9077 \bmod 24257 \\ (2468)^{16} &= (9077)^2 = 15157 \bmod 24257 \\ (2468)^{32} &= (15157)^2 = 20859 \bmod 24257 \end{aligned}$$

So $2468^{47} = (2468)^{32} \times (2468)^8 \times (2468)^4 \times (2468)^2 \times 2468 = 10642 \bmod 24257$.

(c) Here $C = 9625$.

$$\begin{aligned}C \bmod p &= 9625 \bmod 191 = 75 \\a \bmod (p - 1) &= 5603 \bmod 190 = 93\end{aligned}$$

Thus

$$M_1 = 75^{93} \bmod 191 = 20 \text{ (this can be calculated as } 75^{64} \times 75^{16} \times 75^8 \times 75^4 \times 75\text{)}.$$

Also $C \bmod q = 9625 \bmod 127 = 100$ and $a \bmod (q - 1) = 5603 \bmod 126 = 59$.
Thus

$$M_2 = 100^{59} \bmod 127 = 87 \text{ (this can be calculated as } 100^{32} \times 100^{16} \times 100^8 \times 100^2 \times 100\text{)}.$$

Hence we must solve $M = 20 \bmod 191$ and $M = 87 \bmod 127$ using the Chinese Remainder Theorem. Using the Euclidean Algorithm we have

$$\begin{aligned}191 &= 127 + 64 & 1 &= 64 - 63 \\127 &= 64 + 63 & &= 64 - (127 - 64) \\64 &= 63 + 1 & &= 2(64) - 127 \\ & & &= 2(191 - 127) - 127 \\ & & &= 191(2) + 127(-3)\end{aligned}$$

So $191^{-1} \bmod 127 = 2$ and $127^{-1} \bmod 191 = 188$. Thus

$$M = 20(127)(188) + 87(191)(2) \bmod 24257 = 1357$$

so the message was 1357.