Cryptography Exercises

Contents

1 source coding

Problem 1.1. We consider 64 squares on a chess board.

(a) How many bits do you need to represent each square?

(b) In a game on a chessboard one player has to guess where his opponent has placed the Queen. You are allowed to ask six questions which must be answered truthfully by a yes/no reply. Design a strategy by which you can always find the Queen. Show that you can not ensure the exact position when you are allowed to ask five questions.

(c) How do you interpret your result in (b) together with your result in (a)?

Problem 1.2. A language has an alphabet of five letters $x_i,\ i = 1, 2, ..., 5$, each occurring with probability $\frac{1}{5}$. Find the number of bits needed of a fixed-length binary code in which:

(a) Each letter is encoded separately into a binary sequence.

(b) Two letters at a time are encoded into a binary sequence.

(c) Three letters at a time are encoded into a binary sequence.

Which method is efficient in the sense of bit per letter?

Problem 1.3. A language has an alphabet of eight letters $x_i,\ i = 1, 2, ..., 8$, with probabilities $0.25, 0.20, 0.15, 0.12, 0.10, 0.08, 0.05$ and 0.05.

(a) Determine an efficient binary code for the source output.

(b) Determine the average number of binary digits per source letter.

Problem 1.4. Suppose a source outputs the symbols $\{a, b, c, d, e, f, g\}$ with probability $\{0.4, 0.2, 0.1, 0.1, 0.1, 0.05, 0.05\}$.

(a) Give a binary representation for these symbols and calculate the average representation length.

(b) How do you know that your representation has minimum average length?

2 Caesar Cipher

Problem 2.1. We consider a Caesar cipher and assume that the plaintext message is in English. Decrypt the following ciphertext by giving a brief explanation:

$$KNXMNSLKWJXMBFYJWGJSIXFIRNYXB$$
$$TWIKNXMWFSITAJWMJQRNSLFSDIFD$$

Note: Use the following frequency distribution of the letters in the English language for the cryptanalysis:

Table 1:

a	b	c	d	e	f	g	h	i	j	k	l	m
$8,05$	$1,62$	$3,2$	$3,65$	$12,31$	$2,28$	$1,61$	$5,14$	$7,18$	$0,1$	$0,52$	$4,03$	$2,25$
n	o	p	q	r	s	t	u	v	w	x	y	z
$7,19$	$7,94$	$2,29$	$0,20$	$6,03$	$6,59$	$9,59$	$3,1$	$0,93$	$2,03$	$0,2$	$1,88$	$0,09$

(a) What can be the main drawback of the substitution cipher given above?

(b) Caesar cipher is an example of classical cryptosystem. Is this statement true? Why or why not?

(c) Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Take the third letter in each word of the encrypted message above and find the emerging message.

3 Ciphertext-only Attack

Problem 3.1. We consider a ciphertext-only attack on a substitution cipher and assume that the plaintext message is in English. Decrypt the following ciphertext by giving a brief explanation:

$$XTHQTXJSTRFYYJWMTBKFW$$

What can be the main drawback of the substitution cipher given above?

Problem 3.2. We consider a ciphertext-only attack on a substitution cipher and assume that the plaintext is in English. Decrypt the following ciphertext:

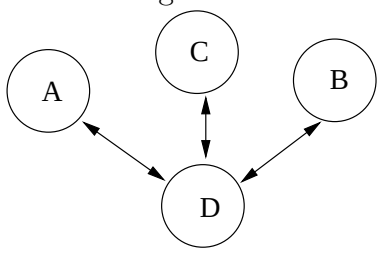
$$ynyqj$$

Hint: Use the frequency distributions of the letters in English language in table 1 for the analysis.

4 Classification of Cryptosystems-Network Nodes

Problem 4.1. Suppose that we have the following network nodes A, B, C and D (Figure 1):

Figure 1:



(a) How many keys do we have to generate such that A, B and C can communicate with D in a bidirectional secure way using a symmetric encryption algorithm?

(b) We replace the symmetric encryption algorithm with a public key system. How many public keys do we have to generate in this case such that A, B and C can communicate with D in a bi-directional secure way?

(c) Suppose that we have 8 nodes in a network. How many symmetric keys do we need such that every pair of nodes can communicate in a safe way?

Problem 4.2. (a) Suppose that we have a network with 10 nodes. How many different keys do we have to generate such that every pair of nodes can communicate in a bi-directional secure way using classical cryptosystem?

(b) We replace classical system with a public key system. How many different keys do we have to generate such that every pair of nodes can communicate in a bi-directional secure way?

(c) Suppose that we extend the network with one more node. How many new extra keys do we need to generate such that every pair of nodes

can communicate in a bi-directional secure way? (Calculate for classical and public cryptosystems).

(d) What is your short conclusion or the interpretation of the results found above?

Problem 4.3. (a) Suppose that we have a network with 6 nodes. How many keys do we have to generate such that every pair of nodes can communicate in a bi-directional secure way using the DES encryption algorithm?

(b) Suppose that we extend the network with one more node. How many new DES keys do we need such that every pair of nodes can now communicate in a safe way?

(c) Instead of DES, we want to use RSA. How many Public keys do we need such that every pair of nodes can now communicate in a safe way?

Problem 4.4. (a) Suppose that we have a network with 6 nodes. How many keys do we have to generate such that every pair of nodes can communicate in a bi-directional secure way using the RSA encryption algorithm.

(b) Suppose that we extend the network with one more node. How many new Public keys do we need such that every pair of nodes can now communicate in a safe way?

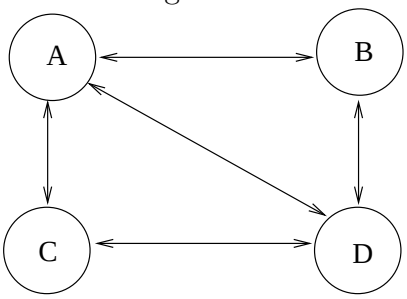
(c) Instead of RSA, we want to use DES. How many keys do we need such that every pair of 7 nodes can communicate in a bi-directional safe way?

Problem 4.5. Suppose that we have the following network nodes: A, B, C, D. Nodes can communicate over the links shown below (Figure 2).

Q1: How many keys do we have to generate such that nodes can communicate over the given links in a bi-directional secure way using the DES encryption algorithm with node A and without node A?

Q2: Instead of DES, we want to use ElGamal public key scheme. How many public keys do we have to generate such that nodes can communicate over the given links in a bi-directional secure way with node A and without

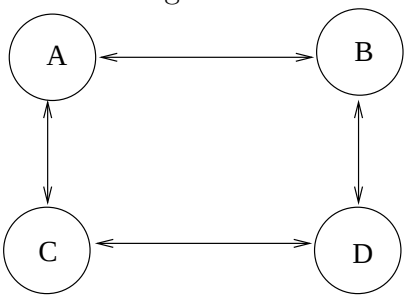
Figure 2:



node A?

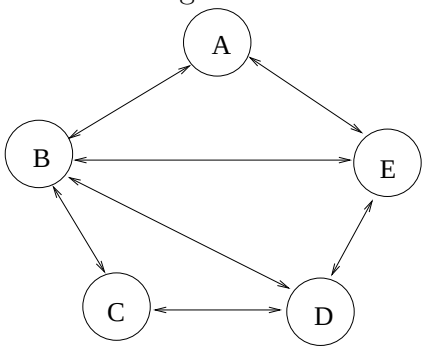
Answer the above questions for the following network nodes (Figure 3):

Figure 3:



Problem 4.6. Consider the figure 4 of a network with nodes A, B, C, D and E. Arrows represent the communication in a bidirectional secure way.

Figure 4:



Q_A) How many keys do we have to generate such that the nodes can communicate over the arrows in a bidirectional secure way using a symmetric encryption algorithm?

Q_B) We replace the symmetric encryption algorithm with a public key system. How many public keys do we have to generate in this case?

5 Properties of modulo Operation

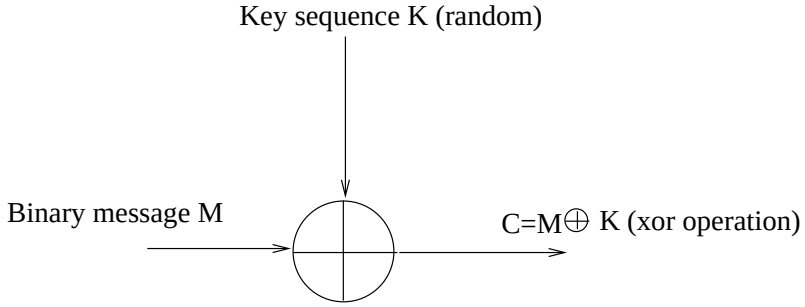
Problem 5.1. Calculate the modulo operations given below:

- $101 \times 98 \; mod \; 17 =$
- $7^5 \; mod \; 15 =$
- $12^8 \; mod \; 7 =$
- $7559 \; mod \; 63 =$
- $-7559 \; mod \; 63 =$
- $7559^{11} \; mod \; 63 =$
- $17^{150} \; mod \; 151 =$
- $14^{10} \; mod \; 197 =$
- $68^{133} \; mod \; 323 =$
- $17^{72} \; mod \; 73 =$
- $7^{73} \; mod \; 71 =$
- $13^{10} \; mod \; 167 =$
- $2^{32} \; mod \; 5 =$
- $8^{64} \; mod \; 9 =$
- $12^{42} \; mod \; 25 =$
- $163 \times 255 \; mod \; 23 =$
- $4^{15} \; mod \; 17 =$

6 Vernam Cipher

Problem 6.1. Consider a Vernam Cipher with the following encryption scheme (Figure 5):

Figure 5:



Assume that a language has only three letters A, B and C. Their binary representations are as follows: $A = 000$, $B = 1111$, $C = 0011$. Two words in the language are encrypted with the same key sequence:

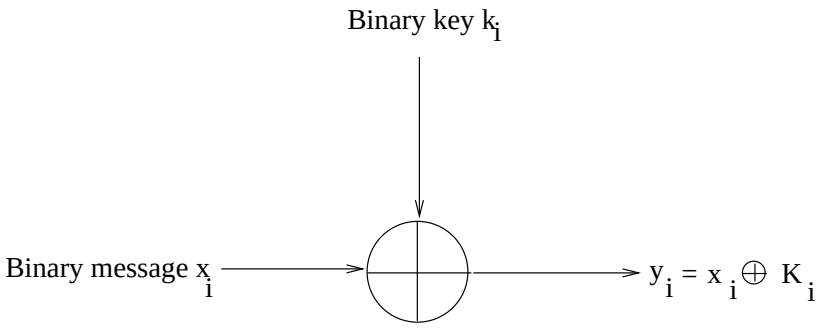
$$W1 = 010100111011101010110010 0$$

$$W2 = 101100101000000000010101 1$$

Determine the possible message pair.

Problem 6.2. The Vernam cipher is an example of a perfect stream cipher (Figure 6):
For the probability $P(k_i = 0) = 0.5$ and $P(x_i = 0) = 0.25$ calculate $P(y_i = 0)$ and $P(y_i = 1)$.
For the probability $P(k_i = 0) = 0.4$ and $P(x_i = 0) = 0.3$ calculate $P(y_i = 0)$ and $P(y_i = 1)$.
For the probability $P(k_i = 0) = 0.5$ and $P(y_i = 0) = 0.25$ calculate $P(x_i = 0)$ and $P(x_i = 1)$.
For the probability $P(k_i = 0) = 0.4$ and $P(y_i = 0) = 0.3$ calculate $P(x_i = 0)$ and $P(x_i = 1)$.
For the probability $P(k_i = 0) = 0.5$ and $P(x_i = 0) = 0.4$ calculate $P(y_i = 0)$ and $P(y_i = 1)$.
For the probability $P(k_i = 0) = 0.4$ and $P(x_i = 0) = 0.4$ calculate $P(y_i = 0)$

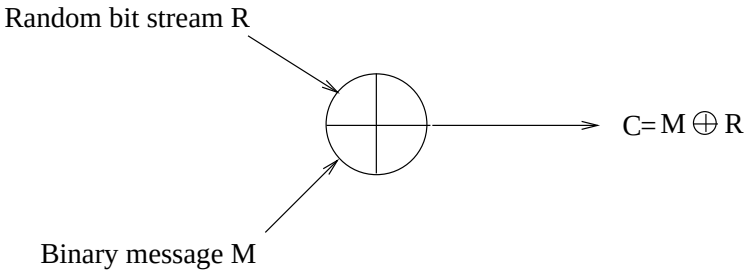
Figure 6:



and $P(y_i = 1)$.
For the probability $P(k_i = 0) = 0.6$ and $P(x_i = 0) = 0.6$ calculate $P(y_i = 0)$ and $P(y_i = 1)$.

Problem 6.3. Suppose that we use the following simple encryption (Figure 7):

Figure 7:



A language has only two words: $A = 111$ and $B = 0000$. Two sentences in the language are encrypted with the same random binary sequence R. The first sentence S_1 is encrypted as 011101101001000111001 and the second sentence S_2 is encrypted as 01101011010100111110. Find good candidates for the original sentences.

Problem 6.4. a) Consider the following letter encodings:

letter	A	E	I	M	O	R	T	V
encoding	000	001	010	011	100	101	110	111

A message $M = MARIO$ is Vernam encrypted into ciphertext $C = AOAMV$; $C = M \oplus K$ where $\oplus$ shows modulo 2 XOR operation. Find the corresponding encryption key. Provide details of your cryptanalaysis.

b) Consider the following two ciphertexts $C_1 = IEEIA$ and $C_2 = ORVRO$ that are obtained from messages M_1 and M_2 respectively under the vernam encryption and the same encryption key. Encrypted messages are two names. Let us denote with $m_{i,k}$ the kth letter in message M_i. The following is known about messages (names): $m_{1,1} = R$ and $m_{2,4} = T$. Using this information, try to recover messages M_1 and M_2, as well as the encryption key. Provide details of your cryptanalysis.

7 Public-Key Algorithms

Problem 7.1. Encrypt the message '**encoding**' using the double Transposition. Choose Key1 and Key2 as '**exam**' and '**study**'.

Problem 7.2. A double transposition cipher uses as first keyword '**exam**' and as second keyword '**topic**'.

Find the plaintext corresponding to the ciphertext $C = isthastties$.

Problem 7.3. Decrypt the ciphertext:

$$HRDYMIPUUNEOBPYEAMTPOAK$$

using Double Transposition with keys $K_1 = CRYPTO$ and $K_2 = MONEY$.

8 Double Encryption

Problem 8.1. We consider double encryption of a private-key algorithm in order to increase the security, such that: $y = e_2(e_1(M))$. Assume two ciphers are given as:

$$\begin{aligned} e_1(x) &= a_1.x + b_1 \\ e_2(z) &= a_2.z + b_2 \end{aligned}$$

where x and z represent the input message, $a_{\{1,2\}}$ and $b_{\{1,2\}}$ are the coefficients.

Show that there is a single cipher $e_3(M) = a_3.M + b_3$ which performs exactly the same encryption (and decryption) as the combination $e_2(e_1(M))$.

9 Vigenere Cipher and Transposition

Problem 9.1. (a) For a transposition cipher the letter frequency remains unchanged. (yes/no)?

(b) The number of different transposition ciphers for a binary word of length 4 is .....

(c) A transposition cipher destroys dependency between letters.

Problem 9.2. Encrypt the message below using the following methods. Assume the English alphabet.

$$Supplieswillarrivetonight$$

1. Vigenere with key=*system*.
2. Double Transposition with key1=*make*, key2=*stand*.

What is the main advantage of Vigenere cipher over Caesar cipher?
What is the main goal of the transposition?
Why is it stronger to apply double transposition instead of single transposition?

Problem 9.3. A Vigenere type of cipher is given as follows:
Plaintext space $X = \{0, \ldots, 25\}$.
Ciphertext space $Y = \{0, \ldots, 25\}$.
Key space $K = \{0, \ldots, 25\}$.
Encryption function is defined by:

$$E(X, K) = (X + K) \ mod \ n.$$

The following alphabet $X = \{A, B, \ldots, Z\}$ are identified with the natural numbers.

(a) Determine the decryption function.

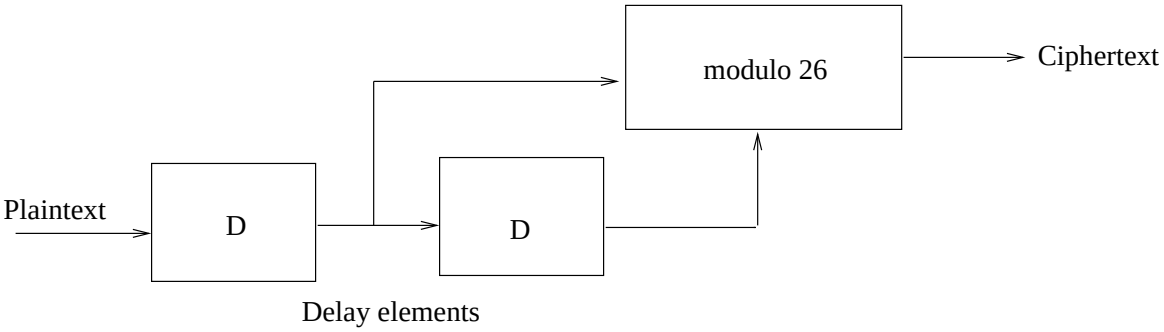
(b) Encrypt the following text by using the key "*hello*" and assuming (as usual) that $n = 26$.

Write your answer with a block of length 5 and ignore spaces, dots and commas. (Show your steps briefly!)

$$Mr.\ President,$$

$$I\ am\ delighted\ to\ accept\ your\ offer.$$

Figure 8:



Problem 9.4. Consider a Vigenere type of cipher with the encryption scheme given in Figure 8.

(a) D represents the delay elements in time where C_i and P_i are the ciphertext and plaintext with the time index i. Write the encryption function from the figure 8.

(b) Determine the decryption function.

(c) Draw the equivalent decryption implementation.

Problem 9.5. Suppose the message

$$SSDTTRRNNRICNAWCOILOATHKIUSGYITATOAAEUN$$

was encrypted using double transposition. Find the keys as well as the plaintext message. Hint: The keys belong to the set

$$\{SYSTEMS, ENGINEERING, UNIVERSITY,$$
$$ESSEN, DUISBURG, CRYPTOGRAPHY\}.$$

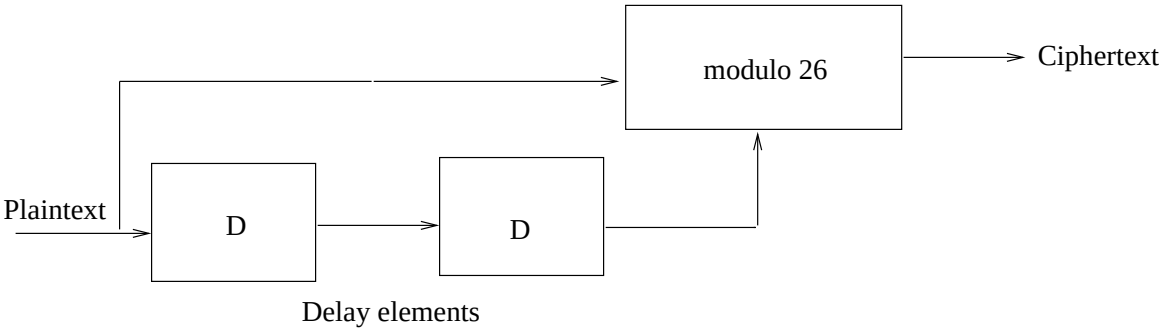
Problem 9.6. A vigenere type of cipher is given by the rule:

$$C_i = P_i + P_{i-2} \ modulo \ 26$$

where C_i and P_i are ciphertext and plaintext symbols at time i, respectively. It is implemented with two delay elements as shown in figure 9.

Give the rule for deciphering and draw the equivalent implementation to decipher the ciphertext.

Figure 9:



Problem 9.7. Decrypt the cipher text $ICPEYDRCTEPDRHIEA$ using the following methods, and the given keys. The alphabet is given by $A = 1$, $B = 2, \ldots, Z = 26$. (Note: The plain text may not be a readable message).

(a) Vigenere (Key = $CRYPTO$).

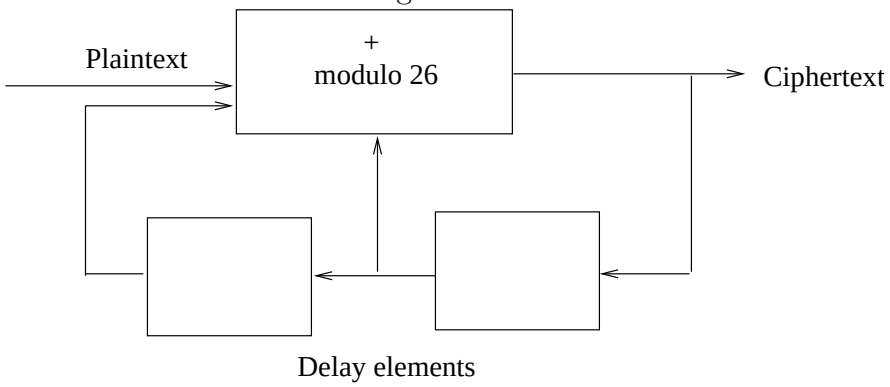
(b) Double Transposition (Key1 = $CRYPTO$, Key2 = $ESSEN$).

Problem 9.8. We consider a Vigenere type block cipher system. You must choose your key according to the last 4 letters of your surname. (Ex: Name: Mengi, Key: engi) Encrypt the following given messages:
1. *spyincountry*
2. *exam*

Hint: A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z. (A=0,.., Z=25).

Problem 9.9. A Vigenere type of cipher is given by the rule: $C_i = (P_i + C_{i-1} + C_{i-2})$ *modulo* 26, where C_i and P_i are ciphertext and plaintext symbols at time i, respectively. It is implemented with 2 delay elements as shown in figure 10:

Figure 10:



Give the rule for deciphering and draw the equivalent implementation to decipher the cipher text.

10 Permutation Cipher

Problem 10.1. Encrypt the message **spyarrivesonthursday** using the double Transposition. Choose Key1 and Key2 as your first and second name. (Ex.: anil mengi, then the Key1=anil and Key2=mengi).

11 Substitution Cipher

Problem 11.1. (a) A substitution cipher destroys dependency between letters. (yes/no?)

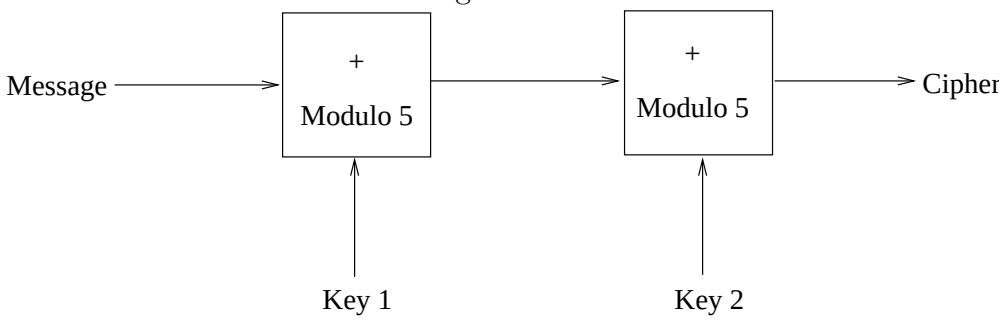
(b) The number of different substitution ciphers for binary words of length 4 is .....

Problem 11.2. In a substitution cipher we replace symbols by other symbols. Suppose that message symbols are elements from the set $\{0, 1, 2, 3, 4\}$. As an example the symbols $\{0, 1, 2, 3, 4\}$ are replaced by $\{0, 4, 1, 2, 3\}$.
Note: we assume that substitution from a set $\{0, 1, 2, 3, 4\}$ to a set $\{0, 1, 2, 3, 4\}$ is also valid.

(a) How many different substitutions are possible for the alphabet with letters $\{0, 1, 2, 3, 4\}$.

(b) Suppose that we implement a substitution system in a double encryption mode as given in figure 11. All the additions are *modulo* 5 addition.

Figure 11:



Given the message $'2'$ and the corresponding cipher $'4'$, what are the possible different keys?

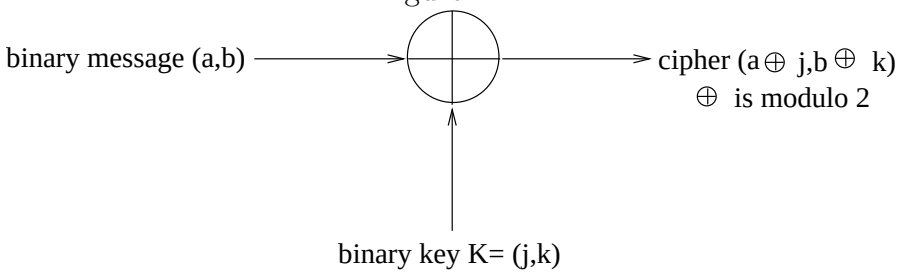
Problem 11.3. In a substitution cipher we replace symbols by other symbols. As an example the symbols $\{00, 01, 10, 11\}$ are replaced by $\{01, 10, 00, 11\}$.

(a) How many different substitution ciphers are possible for binary words of length 2?

(b) The simple substitution ciphers can be realized with a table lookup, where rows correspond to messages and columns to keys. The entries in the table are the ciphers.
What is the size of your table?

(c) Suppose that we implement the substitution in simple way (Figure 12):

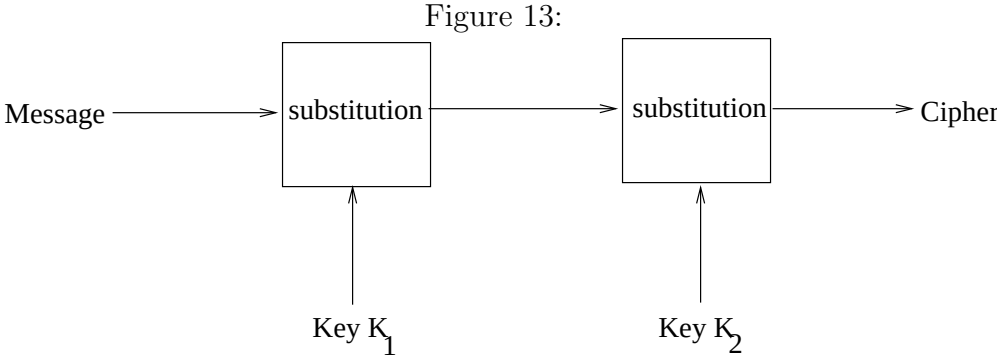
Figure 12:



How many different substitutions are possible for this simple encryption?

(d) We use this simple substitution cipher in a "double encryption" mode (Figure 13):

Figure 13:



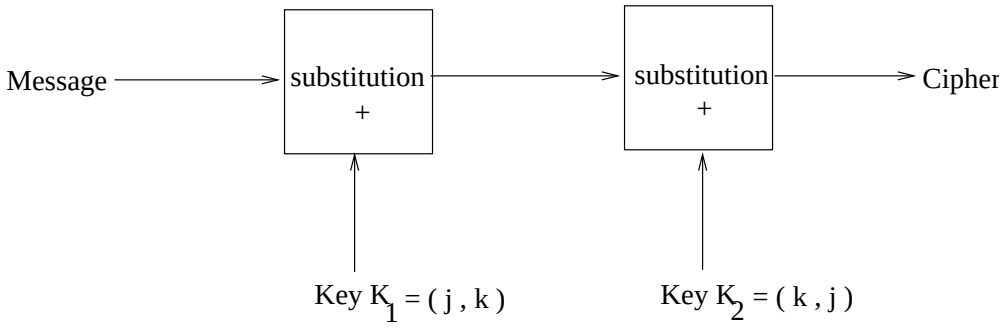
Given the message $(0, 1)$ the corresponding cipher is $(1, 1)$.
How many different solutions are possible for the key pair (K_1, K_2)? Give an example.

Problem 11.4. In a substitution cipher we replace symbols by other symbols. Suppose that message symbols are elements from the set $\{0, 1, 2, 3\}$. As an example the symbols $\{0, 1, 2, 3\}$ are replaced by $\{1, 0, 3, 2\}$.

(a) How many different substitutions are possible for the alphabet with letters $\{0, 1, 2, 3\}$? Suppose that we implement the substitution in a simple way using key symbols from the set $\{0, 1, 2, 3\}$.

(b) We use the substitution cipher in a "double encryption" mode as shown in figure 14:

Figure 14:



Given the message $(1, 2)$ and the corresponding cipher $(3, 0)$, what is the number of possible keys? Give an example of a key $K_1 = (j, k)$.

Problem 11.5. Given is the following string of ciphertext which was encrypted with substitution cipher:

$$asvphgyt$$

The encryption rule is given as

$$C = (M + K) \ mod \ 26$$

where C is the ciphertext, M is the plaintext and K is the key. We assume that the plaintext is in English. You know that the first plaintext letter is a W. Find the key and decrypt the message.

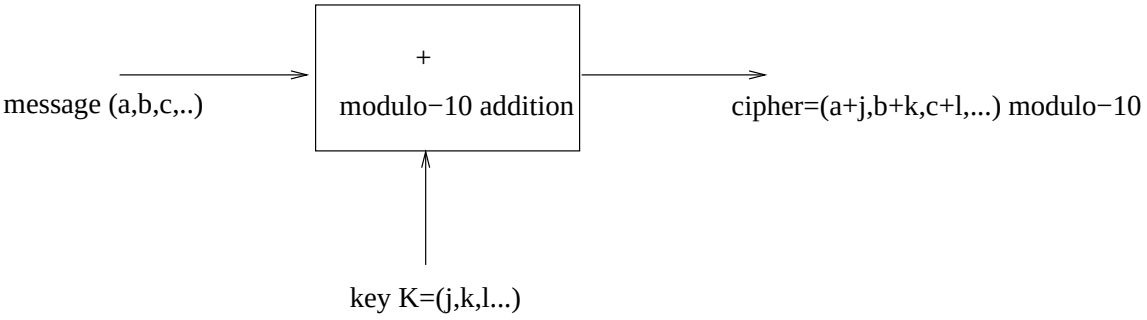
Problem 11.6. In substitution cipher, we replace symbols by other symbols. The message and the key symbols are elements from the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. As an example the symbols $\{0, 6, 5, 2, 4, 0\}$ are replaced by $\{1, 2, 3, 4, 5, 1\}$.

(Q1) How many different substitutions are possible for the alphabet with letters $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Suppose that we implement the substitution in a simple way as given in figure 15. Key is given as $\{8, 5, 4, 6, 8, 2\}$. Assume that the message is the last 6 numbers of your matriculation number. (Ex.: m.n.= 1457652, then the message=$\{4, 5, 7, 6, 5, 2\}$).

(Q2) Calculate the cipher.

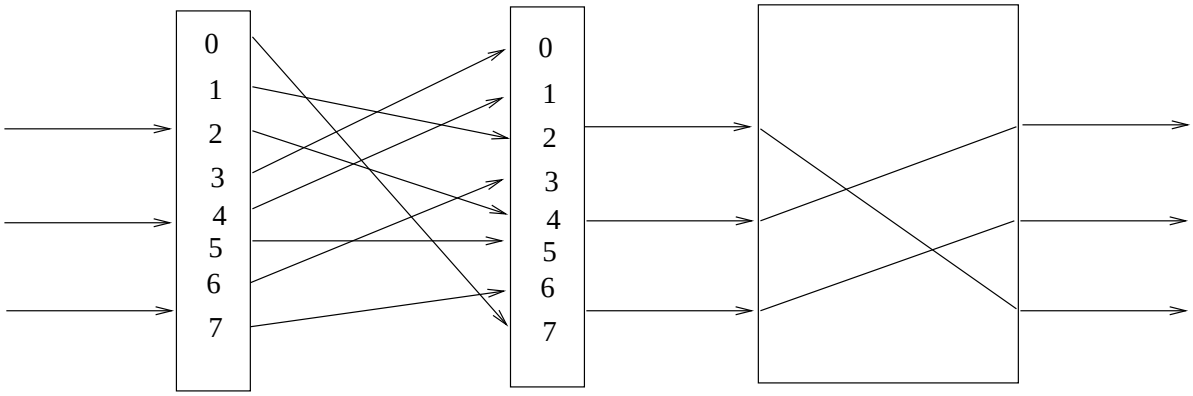
Figure 15:



12 Substitution + Transposition

Problem 12.1. Suppose that we have a binary-to-octal and octal-to-binary substitution followed by a binary transposition scheme as shown in figure 16:

Figure 16:



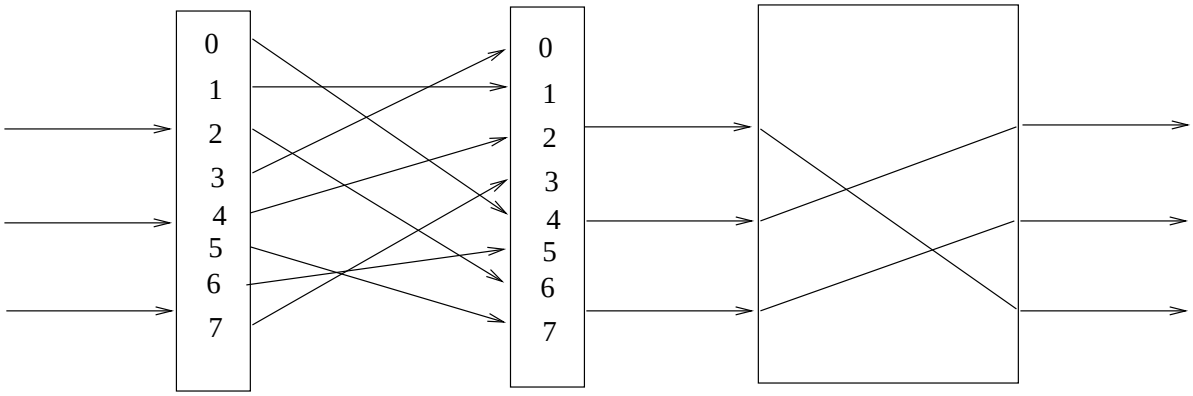
(a) How many different schemes can we construct by changing the mapping of the substitutions and transpositions?
Hint: the order should be the same, i.e. Binary-to-octal and octal-to-binary substitution followed by a binary transposition scheme.

(b) Assume a language with 8 letters: A, B, D, K, M, O, S, T where the decimal representation is $A = 0$, $B = 1$, ..., $T = 7$. In order to encrypt a letter in this language, we convert the letter in binary form, apply the scheme above and convert them back into the corresponding letter. Encrypt the given word: $BOSTAK$.

Problem 12.2. Suppose that we have the binary-to-octal and octal-to-binary substitutions followed by a binary transposition scheme shown in figure 17:

Q1: How many different schemes can we construct by changing the substitutions and transpositions? (The order should be the same: Binary-to-octal and octal-to-binary substitutions followed by a binary transposition.)

Figure 17:



Q2: Assume a language with 8 letters: A, B, C, K, L, O, T, Y. In order to encrypt a word in this language, we convert the letters into binary form, apply the scheme above and convert them back to corresponding letters. Encrypt the word: KAL.

Hint: A=0, B=1, C=2, K=3, L=4, O=5, T=6, Y=7.

13 Affine Cipher

Problem 13.1. We consider the affine code that transforms a message M into ciphertext C as

$$C = (19.M + 6) \; mod \; 31.$$

In other words, M is multiplied with 19, 6 is added to the sum and modulo 31 is taken over the result.

(Q_1) Encrypt M=29.

(Q_2) The message can be recovered by an affine transformation of the form

$$M = (a.C + b) \; mod \; 31.$$

Determine the constants a and b.

Problem 13.2. The encryption for 128 different symbols is given by the following equation:

$$C = (K_1 \times M + K_2) \; modulo \; 128;$$

where C and M represent the cipher and the message, respectively.

Q1: For $K_1 = 11$ and $K_2 = 17$, encrypt $M = 70$.

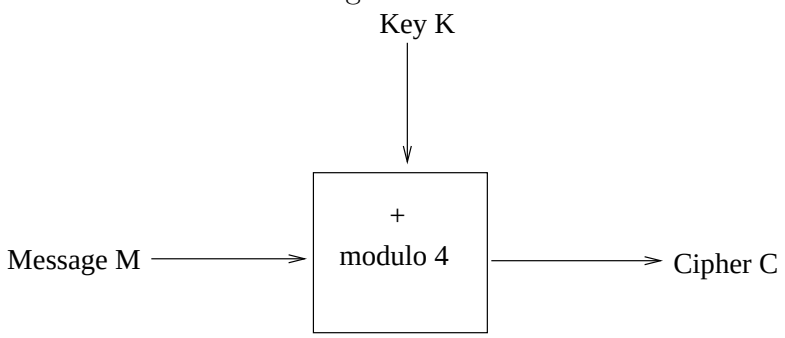
Q2: Find the corresponding decryption function.

Q3: Give the message that follows from $C = 20$ for the same K_1 and K_2 values.

14 Perfect Secrecy

Problem 14.1. Consider the cryptosystem with probability measures given in figure 18:

Figure 18:



where:

(i) $K \in \{0, 1, 2, 3\}$ and $P(K = 0) = 1/3,\ P(K = 1) = P(K = 2) = 1/6$.

(ii) $M \in \{0, 1, 2, 3\}$ and $P(M = 0) = 1/7,\ P(M = 1) = 3/7$ and $P(M = 2) = 2/7$.

(iii) $C = (M + K)$ *modulo* 4.

(a) Calculate the corresponding probabilities: $P(M = 3),\ P(K = 3),\ P(C = 0),\ P(C = 2),\ P(C = 2|M = 0),\ P(C = 0|M = 0)$.

(b) What is the condition for perfect secrecy?

(c) Does this cryptosystem provide perfect secrecy? Prove your answer mathematically.

Problem 14.2. Consider the cryptosystem with probability measures given as follows:

- Plaintext space $X = \{a, b, c\}$.
- Ciphertext space $Y = \{1, 2, 3, 4\}$

- Key space $K = \{K_1, K_2\}$

Encryption functions are defined by:

	a	b	c
K_1	1	2	3
K_2	2	3	4

Plaintext and key distributions are defined by:

a	b	c
1/4	1/4	1/2

K_1	K_2
1/4	3/4

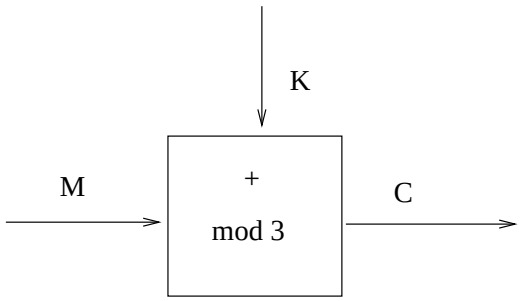
(a) What is the condition for perfect secrecy?

(b) Compute the corresponding probability measures on ciphertext ($P(Y = i), i = 1, 2, 3, 4$).

(c) Check and prove whether this cryptosystem is secure.

Problem 14.3. A ternary source generates symbols $M = \{0, 1, 2\}$ with probability $P(M = 0) = \frac{1}{2}$, $P(M = 1) = P(M = 2) = \frac{1}{4}$. Consider two substitution ciphers given in A and B.

Figure 19:



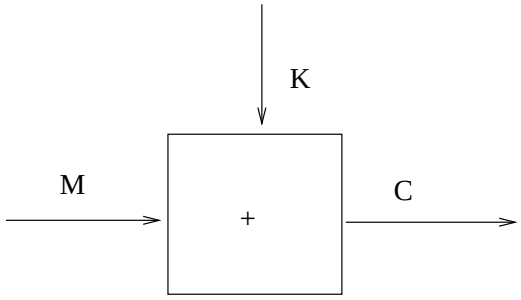
(A) We use a substitution cipher with an encryption rule $C = (M + K)$ *mod* 3 (Figure 19), where $K \in \{0, 1\}$ is the key with the probability $P(K = 0) = P(K = 1) = 1/2$ and $C \in \{0, 1, 2\}$ is the ciphertext. Answer the following questions:

(a) Calculate $P(M = 0|C = 0)$ and $P(C = 2)$.

(b) Does this scheme provide perfect secrecy? Motivate your answer mathematically!

(B) Another substitution cipher calculates $C = M + K$ (Figure 20), where now $C \in \{0, 1, 2, 3\}$ and $K \in \{0, 1\}$ with the probability $P(K = 0) = P(K = 1) = \frac{1}{2}$. Answer the following questions:

Figure 20:

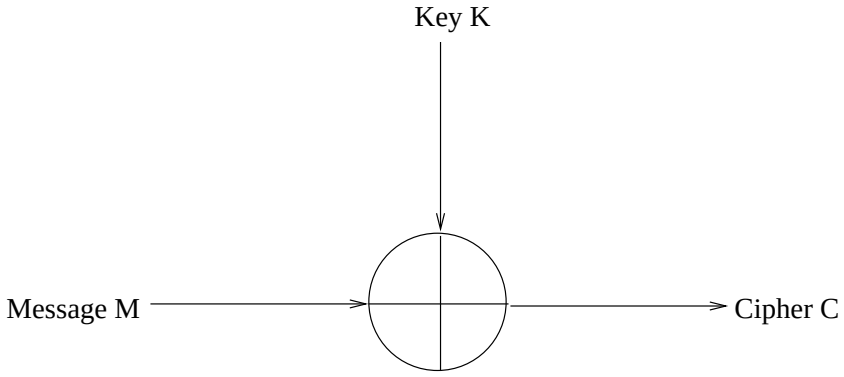


(c) Calculate $P(M = 0|C = 0)$ and $P(C = 2)$.

(d) Which scheme A or B gives better security? Why?

Problem 14.4. Consider the cryptosystem given in figure 21:

Figure 21:



Where:

- $M \in \{0,1\}$,
- $K \in \{0,1\}$: $P(K=0) = P(K=1) = \frac{1}{2}$,
- $C = M \bigoplus K$

(a) For a given probability $P(M=0) = \frac{1}{3}$ and $P(M=1) = \frac{2}{3}$, calculate the following probabilities:
$P(C=0) = \ldots\ldots$,
$P(M=0|C=0) = \ldots\ldots$.

(b) Does this cryptosystem provide perfect secrecy? Prove your answer mathematically!

Problem 14.5. Suppose that a sender and receiver use the encryption table in figure 22:

Figure 22:

	key			
Message	00	01	10	11
x = 0	0	1	3	2
x = 1	2	0	1	3

cipher

We assume further that the keys are selected with equal probability and $P(X=0) = 1 - P(X=1) = \frac{1}{3}$.

(a) A passive attacker observes the cipher 3. What is the probability that the transmitted message is 1, given the observed cipher is 3?

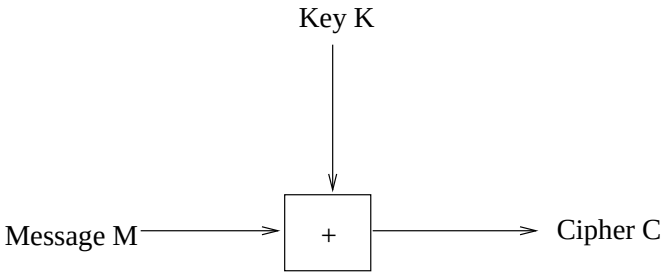
(b) An active attacker changes an observed cipher 3 with 1. What is the probability that this cipher is accepted as valid by the receiver?

(c) An active attacker injects the cipher 3. What is the probability that this cipher is accepted as valid by the receiver?

Problem 14.6. Suppose that we have the encryption scheme in figure 23: where

(i) $M \in \{0,1,2\}$ and $P(M=0) = P(M=1) = P(M=2) = \frac{1}{3}$,

Figure 23:



(ii) $K \in \{0,1\}$: $P(K=0) = P(K=1) = \frac{1}{2}$,

(iii) $C = M + K$ *modulo* 3

Calculate the following probabilities:

(a) $P(C=0) = \ldots\ldots$

(b) $P(M=0|C=0) = \ldots\ldots$

Problem 14.7. Consider the cryptosystem with probability measures given as follows:

$P(K_1)$	$P(K_2)$	$P(K_3)$	$P(a)$	$P(b)$
1/4	1/2	1/4	1/4	3/4

Encryption function is given as:

	a	b
K_1	1	2
K_2	2	3
K_3	3	4

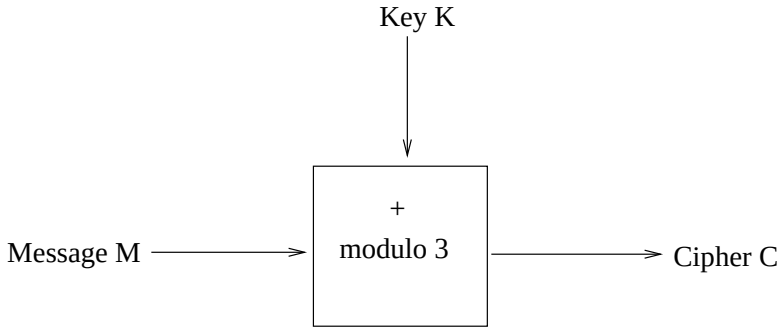
Answer the following questions:

- $P(1) = \ldots\ldots$
  $P(2) = \ldots\ldots$
  $P(3) = \ldots\ldots$
  $P(4) = \ldots\ldots$
- Write down the condition for perfect secrecy.

- Is this cryptosystem secure? Why or why not?

Problem 14.8. Consider the cryptosystem with probability measures given in figure 24:

Figure 24:



- $K \in \{0, 1, 2\}: \ P(K = 0) = 1/5, \ P(K = 1) = P(K = 2) = 2/5.$
- $M \in \{0, 1, 2\}: \ P(M = 0) = 1/7, \ P(M = 1) = 4/7.$
- $C = (M + K)$ *modulo* 3

Q1: Calculate the following probabilities:
$P(M = 2) = \ldots\ldots$
$P(C = 0) = \ldots\ldots$

Q2: Write down the condition for perfect secrecy.

Q3: Does this cryptosystem provide perfect secrecy? Prove your answer mathematically!

Problem 14.9. Suppose that a sender and receiver use the following encryption table:

	M_1	M_2
K_1	1	2
K_2	2	3
K_3	2	4
K_4	3	2
K_5	4	1

where M and K represent the message and the key, respectively. Let the keys be selected with equal probability. Probability distribution of the messages is not known. For each transmission the ciphertext is valid for the particular key which is known by both sides. Assume that an attacker knows the encryption table.

(Q_1) Show mathematically that whether this system does provide perfect secrecy or not.

(Q_2) An attacker changes an observed cipher 2 by the value 1. The probability that this cipher is accepted as valid by the receiver.

(Q_3) An attacker changes an observed cipher 3 by the value 2. The probability that this cipher is accepted as valid by the receiver.

Problem 14.10. Suppose that a sender and receiver use the following encryption table:

	M_1	M_2
K_1	1	2
K_2	2	3
K_3	3	4
K_4	4	1

where M and K represent the message and the key respectively. We assume further that the keys and the messages are selected with probability $P(M_1) = 1/4$, $P(M_2) = 3/4$, $P(K_1) = 1/2$ and $P(K_2) = P(K_3) = 1/6$.

(Q_1) Show mathematically that the given system does not provide perfect secrecy.

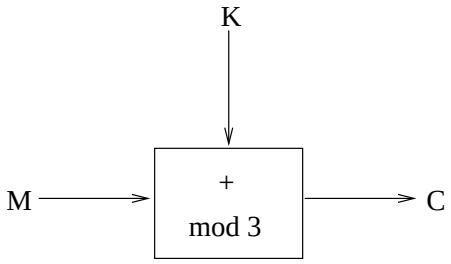
(Q_2) Modify plaintext and/or key distribution in such a way that perfect secrecy is obtained. Explain your choice.

Problem 14.11. Consider the cryptosystem in figure 25 with probability measures given as follows:

Key $K \in \{0, 1, 2\} : P(K = 0) = 3/5, P(K = 1) = P(K = 2) = 1/5,$

Message $M \in \{0, 1, 2\} : P(M = 0) = 3/7, P(M = 1) = 2/7,$

Figure 25:



Cipher $C = (M + K)$ *modulo* 3.

Q1: Calculate the following probabilities.
$P(M = 2) = ...$ $P(C = 0) = ...$

Q2: Write down the condition for perfect secrecy.

Q3: Does this cryptosystem provide perfect secrecy? Prove your answer mathematically!

Problem 14.12. Suppose that a sender and receiver use the following encryption table:

	K_1	K_2	K_3	K_4	K_5
M_1	1	2	3	3	4
M_2	2	3	4	3	1

where M and K represent the message and the key, respectively. Let the keys be selected with equal probability. The probability distribution of the message is not known. The key and the message determine the ciphertext. **Assume that the particular key and the encryption table are known by both sides.**

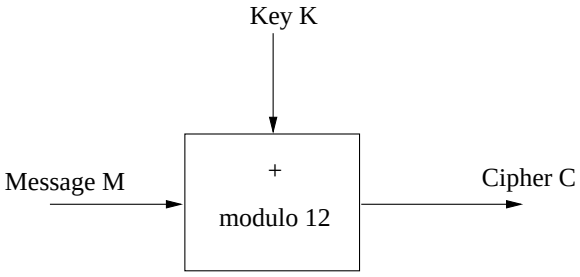
(Q_1) Show mathematically whether this system provides perfect secrecy or not.

(Q_2) An attacker changes an observed cipher 4 by the value 1. Give the probability that this cipher is accepted as valid by the receiver.

(Q_3) An attacker changes an observed cipher 3 by the value 1. Give the probability that this cipher is accepted as valid by the receiver.

Problem 14.13. Consider the last 3 numbers of your matriculation number. For the simplicity, the last 3 numbers will be denoted as $\{mat_1, mat_2, mat_3\}$. (Ex.: m.n.= 1457652, then the message=$\{mat_1 = 6, mat_2 = 5, mat_3 = 2\}$).

Figure 26:



Consider the cryptosystem given in figure 26 where the message and the key are the elements from a set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. The probability distribution of the message is given as follows,

M	0	1	2	3	4	5	6	7	8	9
p(M)	3/10	1/10	1/10	3/20	1/20	1/40	1/10	1/10	1/20	1/40

Keys are equally distributed. Cipher C is calculated as follows,

$$C = (M + K) \ \ modulo\ 12. \tag{1}$$

(Q_1) Calculate the following probabilities:

$P(C = mat_3) =$
$P(C = mat_2|M = 2) =$
$P(M = 5|C = mat_1) =$

(Q_2) What is the condition for perfect secrecy?

(Q_3) Prove mathematically whether this system provides perfect secrecy or not?

Problem 14.14. The encryption/decryption of a sequence of letters from the alphabet $\{A, B\}$ into a cipher with letters $\{a, b, c\}$ is done according to the following table.

Key	A	B
1	a	b
2	b	c
3	b	a
4	c	b

The key letters $\{1, 2, 3, 4\}$ have equal probability. An unauthorized person knows the table and can observe and modify the ciphertext. A modification is successful if the receiver accepts the modified cipher symbol, i.e. the ciphertext is valid for the particular key.

Example: at time i: plaintext $P_i = B$ and $K_i = 3$ gives $C_i = a$.
A modification may change a into b for a given $K_i = 3$.

Q1: Does the cipher provide perfect secrecy? YES/ NO?

Q2: What is the probability of successful modification for an observed cipher b?

$P(\text{success}|\text{observed cipher}= b) =$

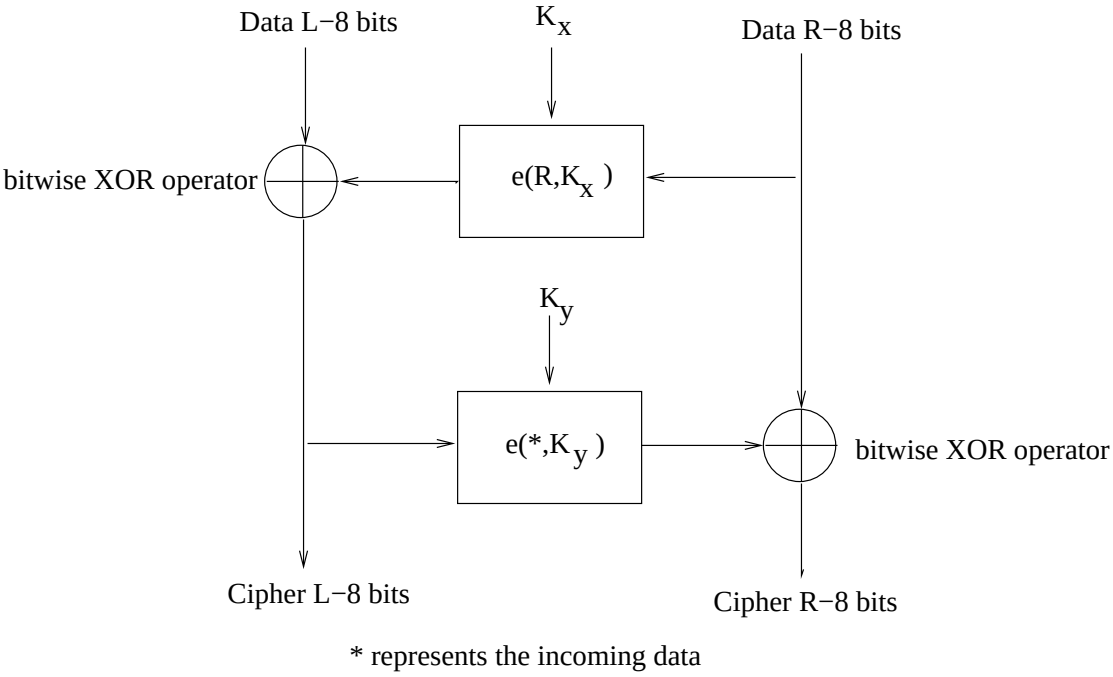
Q3: What is the probability of successful modification for an observed cipher a?

$P(\text{success}|\text{observed cipher} = a) =$

15 Feistel Cipher

Problem 15.1. Consider the Feistel network structure in figure 27:

Figure 27:

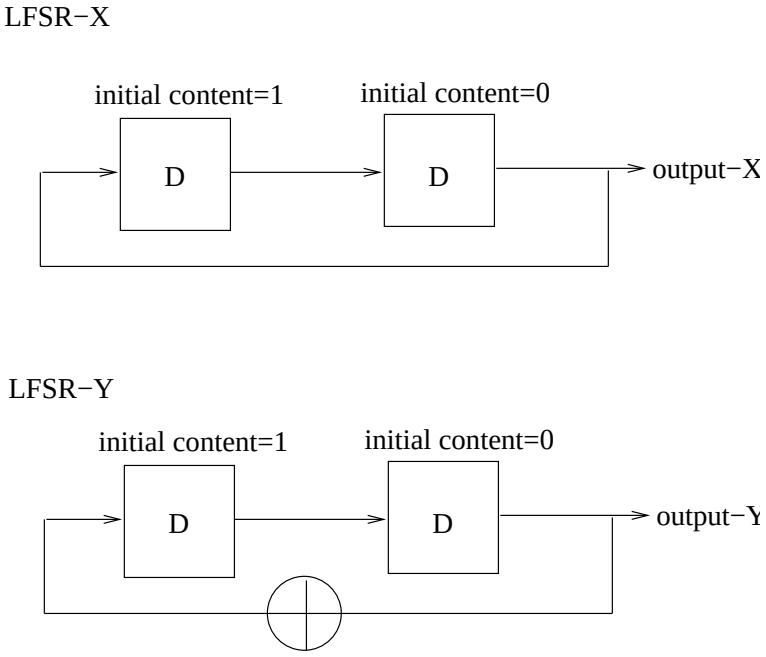


(a) Write down the general mathematical expression for the outputs; cipher-L and cipher-R.

(b) Linear feedback shift registers are used to generate random binary sequences. Consider the two LFSRs in figure 28 where 'D' represents the delay elements. For an initial content (seed) of 1 and 0 for both LFSR's, write down the output sequences. (at least 8 bits.)
Hint: first output should be the first bit of the sequence.

(c) Consider again the Feistel Cipher. Encryption is done by simple XOR operation. We use LFSR-X to generate key sequence Kx (8 bits) and LFSR-Y to generate key sequence Ky (8 bits). Use the first 8 bits

Figure 28:

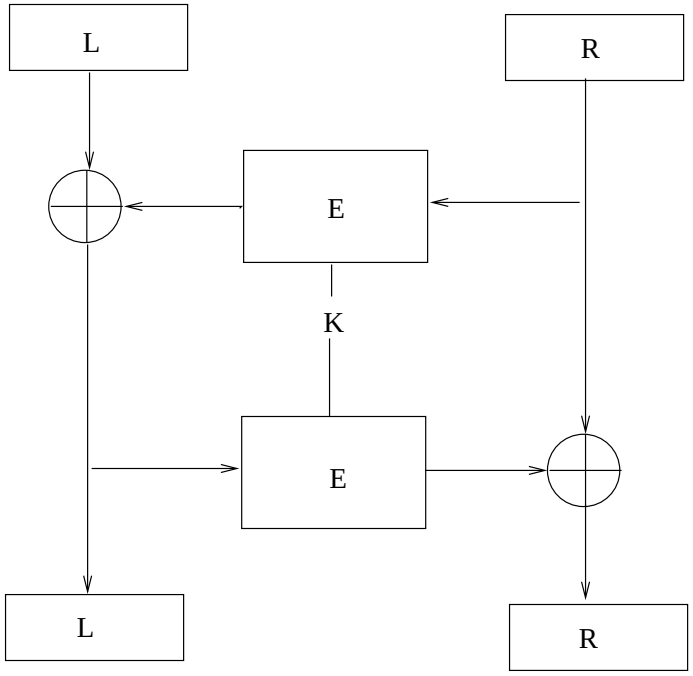


output of LFSR-X and LFSR-Y and calculate the output bit sequences; cipher L and cipher R where the inputs are given as follows:

Data L= 10111010 Data R= 10010101.

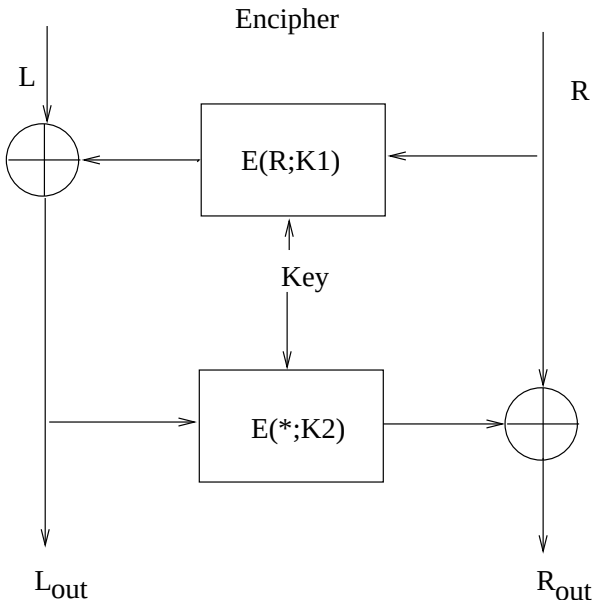
Problem 15.2. Calculate the output of the Feistel-Network in figure 29 given the input 01101011010111011010001111010101 and the key 0111010010101001. Assume that the left and right parts are 16 bits each and that the encryption function is an exclusive-OR (XOR).

Figure 29:



Problem 15.3. Consider the Feistel network structure in figure 30.

Figure 30:

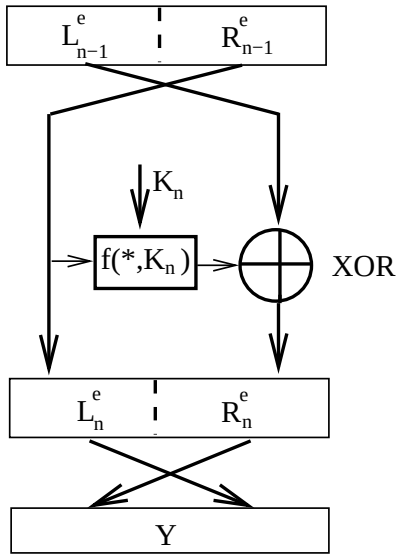


Q1: Calculate L_{out} and R_{out} for the given system above.

Q2: Draw the decryption scheme.

Problem 15.4. Consider the Feistel network in figure 31. Superscript ^{e} denotes the encryption process and f represents the encryption function with the key.

Figure 31:

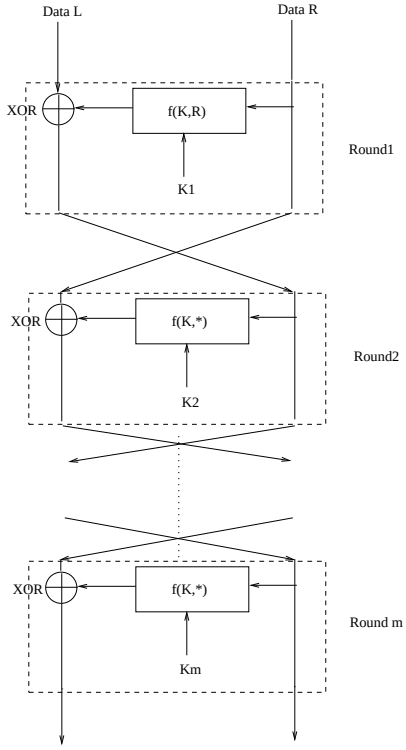


Q1) Express L_n^e and R_n^e through values L_{n-1}^e and R_{n-1}^e .

Q2) Given is the last round of an n-round Feistel network in figure 31. Draw the first round of the corresponding decryption network. Use superscripts ^{d} to denote the decryption process.
Hint: In Feistel networks, the encryption and decryption are almost identical operations.

Problem 15.5. Consider an m-round Feistel network as given in figure 32. Assume that all subkeys are equal, i.e. $K1 = K2 = .. = Km$ and with a subkey size half of the block size. The encryption function $f(K, R) = K \oplus R$.

Figure 32:



Analyze how (in)secure this cipher is against ciphertext only attacks and known plaintext attacks when

(Q_1) $m = 2$.

(Q_2) $m = 3$.

(Q_3) m is arbitrary.

Problem 15.6. Consider figure 32. Assume a simple two round Feistel block cipher with an eight bit key and 16 bit block size. Key derivation is defined as $Ki = \mathbf{K}_{(dec)} + 89.i \ mod \ 256$ where Ki is the ith subkey and $\mathbf{K}$ is

the decimal representation of the key. The encryption function $f(Ki, Ri) = 127.(Ki_{(dec)} + R(i-1)_{(dec)})\ mod\ 256$ where $R(i-1)$ represents the input of the block as seen in the figure.

(Q_1) Encrypt the last 2 letters of your surname (ex: surname:mengi, message: (g i)). Use ASCII table in Chapter 1 slide 8 to transform the letters into other representations. The key **K** is given as $55_{(hex)}$.

(Q_2) How is decryption affected if the ciphertext is modified due to the transmission errors?

16 Block Cipher

Problem 16.1. Let a block cipher with secret key K be chained in the following way:

$$C_i = M_{i-1} \oplus E((M_i \oplus C_{i-1}), K) \qquad \text{for } i > 0$$

where M_0 and C_0 are fixed public initialization vectors, K is the secret key known to both transmitter and receiver, and E and D represent encryption and decryption, respectively.

Q1) Determine the equation for decryption and draw the block diagram.

Q2) Suppose that ciphertext C_3 is damaged in transmission. Which plaintext blocks become undecipherable as a result? Explain.

Problem 16.2. A block cipher uses the recurrence

$$C_i = E((M_i \oplus C_{i-1}), K), \quad i > 0$$

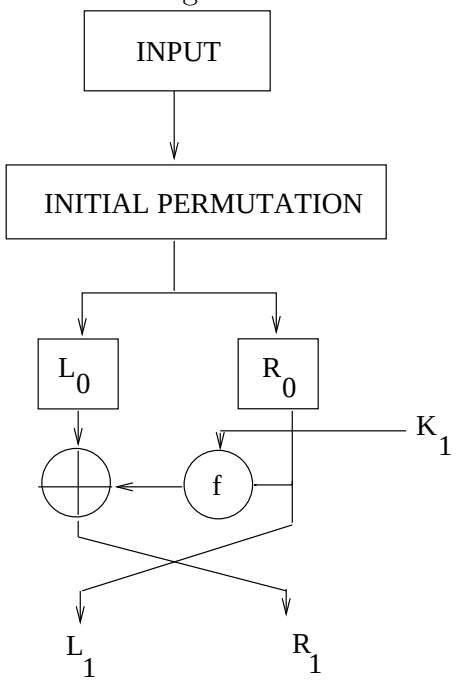
where $M_1 M_2 M_3 ...$ is the message, C_0 is a randomly chosen initial vector, K is the secret key known to both transmitter and receiver, and E and D represent encryption and decryption, respectively.

Determine the equation for decryption and draw the block diagram.

17 Digital Encryption Standard (DES)

Problem 17.1. We consider a DES-based encryption scheme, which operates on 16-bit blocks of plaintext and uses sub-key of length 12. A sketch of the encryption with first-round is given in figure 33:

Figure 33:



Consider the following bit sequence as the input data:

1011000110101100

(a) Describe L_1 and R_1 with respect to R_0, R_1 and K_1.

(b) The 16 bits of the input are first reorganized by the following initial permutation (IP).

8	13	4	9
16	5	12	1
7	14	3	10
15	6	11	2

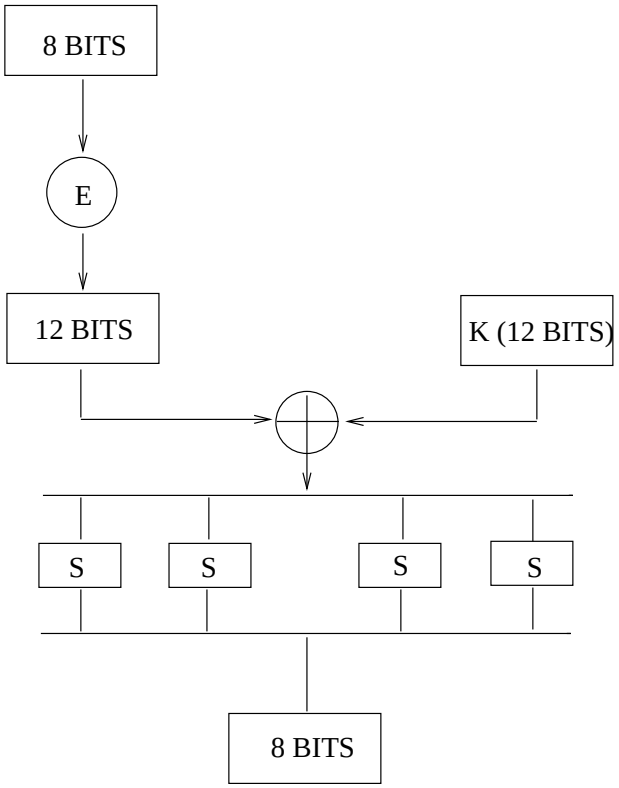
That is the permuted input has bit 8 of the input as its first bit, bit 13 as its second bit and so on.

(i) Write down the permuted input.

(ii) Compute the inverse permutation namely IP^{-1}.

(c) Let the 16 bits of the permuted input block consist of an 8 bit block L followed by an 8 bit block R. The internal structure of the cipher function f (see f in figure 33) is given in figure 34.

Figure 34:



E denotes an expansion function which takes a block of 8 bits as input and yields a block of 12 bits as output according to the table given below. (The first two bits of output are the bits in position 8 and 2

and so on.)

$$\begin{matrix} 8 & 2 & 4 \\ 1 & 3 & 2 \\ 6 & 1 & 7 \\ 5 & 3 & 8 \end{matrix}$$

Write down the expanded output.

(d) S denotes the substitution function which takes a block of 3 bits and yields a block of 2 bits. Function is given with a table which contains the decimal representations.

(ex: $(101)2 = 5$, so from the table, 5 corresponds to 3 which is $(11)2$.)

0	1	2	3	4	5	6	7
1	3	2	1	0	3	0	2

Write down the output bit sequence with a given sub-key $K1 = 101101100010$.

(e) Write down $L1$ and $R1$ as a bit sequence.

(f) Combine $L1$ and $R1$ into 16-bits bit sequence and apply the inverse permutation (IP^{-1}).

Problem 17.2. We consider a Cipher-Block Chaining Mode (CBC mode) for a block cipher which implements the encryption as $C_i = E(M_i \oplus C_{i-1}, K)$ for $i > 0$ where $M_1 M_2 M_3 \ldots$ is the message and C_0 is a randomly chosen initial vector.

(i) Explain (with motivation) how decryption is done.

(ii) How does a bit error in the ciphertext influence decryption? (Assume that C_i is obtained corrupted because of a bit error. How does it effect the next decryption steps?)

Problem 17.3. Encryption of large blocks using DES (or any fixed size block cipher) can be achieved through the means of modes. For three modes, the encryption is depicted in figures 35, 36 and 37. Draw the decryption block diagram of each of these modes, and give the mathematical expression for the first two of them. What are the advantages and disadvantages of each of the three modes?

Figure 35: Electronic Codebook (ECB)

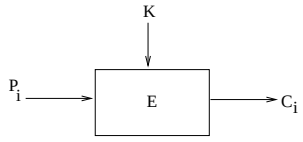


Figure 36: Cipher Block Chaining (CBC)

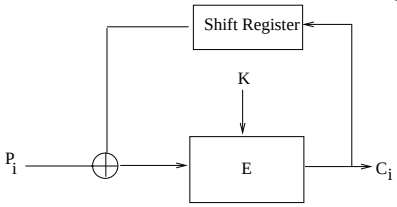
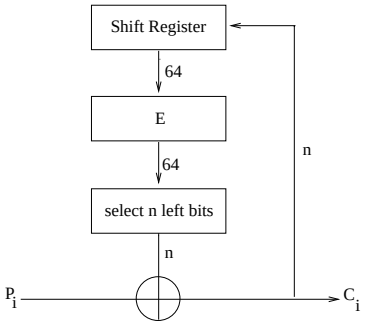


Figure 37: Cipher Feedback (CFB) ($n \leq 64$)



Problem 17.4. Suppose that we use DES in cipher block chaining mode.
The encryption rule for message M_i, key K and cipher C_{i-1} is:

$$C_i = DES(M_i \oplus C_{i-1}, K) \; i = 1, 2, \ldots$$

where C_0 is an initial block and $\oplus$ the component-wise modulo-2 operation (XOR).

(i) What is the decryption rule? $M_i = \cdots\cdots\cdots$

(ii) Suppose an attacker changes C_i into $C_i' \neq C_i$. How many messages are then decrypted incorrectly?

Problem 17.5. Suppose that we use DES in counter mode.
The encryption rule for key K and message M_i, at time $i > 0$ is:

$$C_i = DES(R_i, K) \oplus M_i, \qquad R_i = R_{i-1} + 1$$

where R_0 = some starting value and $\oplus$ the component-wise modulo-2 operation (XOR).

(i) What is the decryption rule? $M_i = \cdots\cdots\cdots$

(ii) Suppose an attacker changes C_i, into $C_i' \neq C_i$. How many messages are then decrypted incorrectly?

Problem 17.6. Suppose that we use DES in cipher feedback mode.
The encryption rule for message M_i, key K and cipher C_{i-1} is:

$$C_i = M_i \oplus DES(C_{i-1}, K) \; i = 1, 2, \ldots$$

where C_0 is an initial block and $\oplus$ the component-wise modulo-2 operation (XOR).

(i) What is the decryption rule? $M_i = \cdots\cdots\cdots$

(ii) Suppose an attacker changes C_i, into $C_i' \neq C_i$. How many messages are then decrypted incorrectly?

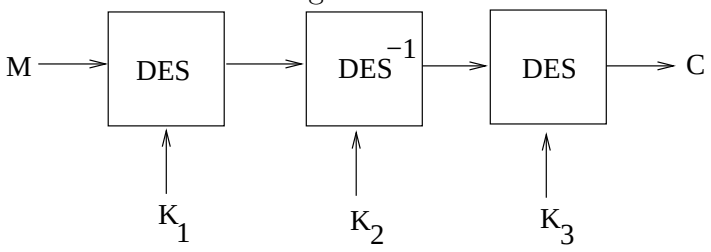
Problem 17.7. Suppose that we encrypt a message M in 3 DES rounds, as indicated in figure 38:

$$C = DES(DES^{-1}(DES(M, K_1), K_2), K_3)$$

Note: when $C = DES(M, K)$, then $DES^{-1}(C, K) = M$.

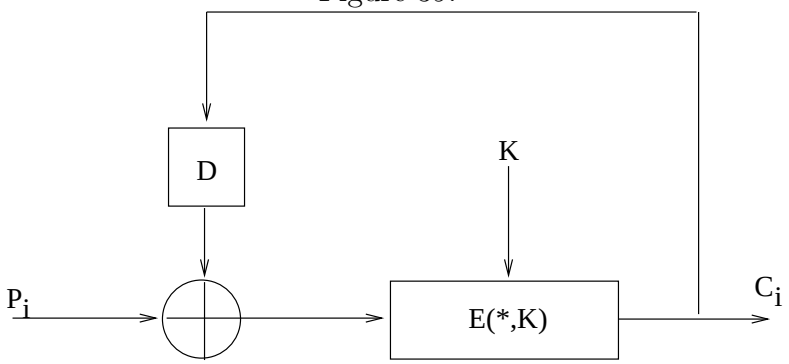
Question: When does this scheme reduce to single DES?

Figure 38:



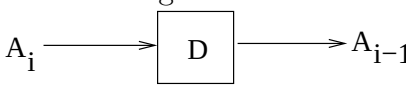
Problem 17.8. For a cipher block-chaining mode, the encryption is depicted in figure 39. Give the mathematical expression of the encryption, decryption and draw the corresponding block diagram.

Figure 39:



(Note: $'D'$ represents delay element.)

Figure 40:



Problem 17.9. We now look at the following variant of key whitening with DES. Suppose that the message M and the keys K_1 and K_2 are 56 bits long. The encryption is defined

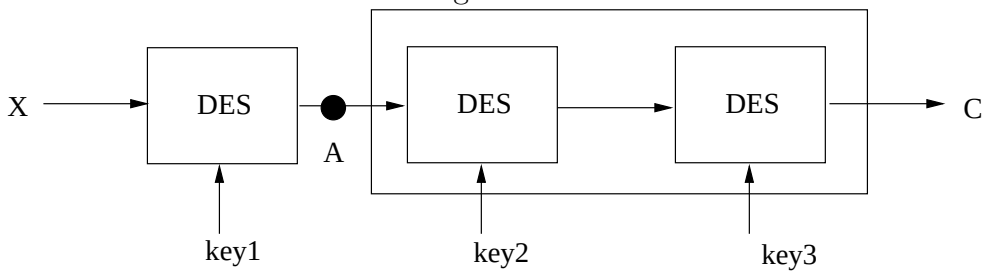
$$C = DES((M \oplus K_1), K_2). \tag{2}$$

Q_A) Show that breaking the scheme above is roughly as difficult as a brute force attack against single DES.
Hint: To get started, it is recommended that you draw a diagram.

Q_B) What is the complexity of known plaintext-cipher (M and C) attack on that scheme?

Problem 17.10. We consider a triple DES structure as given in figure 41 where the key size is 56 bits.

Figure 41:

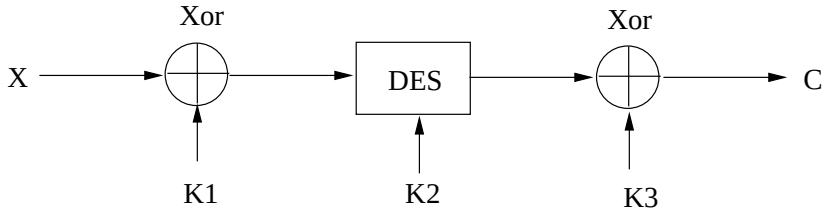


(Q_1) Apply the known plaintext-ciphertext attack at position A. **Describe** your attack.

(Q_2) What is the complexity of your attack?

Problem 17.11. We consider a 'key whitening' scheme as given in the figure 42.

Figure 42:



(Q_1) Describe the encryption function for X.

(Q_2) Describe the decryption function for C.

18 Primitive Element

Problem 18.1. (i) Explain in at most two sentences what a primitive element is.

(ii) Calculate the smallest primitive element for $p = 23$.

Problem 18.2. Find x and y such that the given equation is satisfied.
Hint: use primitive element.

$32\mathbf{x} = 1 \ mod \ 1409.$

$8\mathbf{y} = 9 \ mod \ 13.$

$25\mathbf{x} = 1 \ mod \ 42.$

$18\mathbf{y} = 11 \ mod \ 19.$

$17\mathbf{x} = 1 \ mod \ 81.$

$11\mathbf{y} = 10 \ mod \ 13.$

$8\mathbf{x} = 9 \ mod \ 17.$

$14\mathbf{y} = 1 \ mod \ 17.$

19 Diffie-Hellman Key Exchange

Problem 19.1. Assume that two users want to establish a common secret key over an insecure channel by using Diffie-Hellman key exchange protocol. The private key for user A is 15 and for user B is 10. We consider a commonly known prime 29.

(i) Calculate the smallest primitive element for $p = 29$. (Show your steps clearly.)

(ii) Obtain the common key by using the primitive element found above (Show your steps).

Problem 19.2. Assume that two users want to establish a common secret key over an insecure channel by using Diffie-Hellman key exchange protocol. The private key for user A is 11 and for user B is 14. We consider a commonly known prime 17.

(i) Find the smallest primitive element for $p = 17$ (Show your steps).

(ii) Obtain the common key by using the primitive element found above (Show your steps).

Problem 19.3. Assume two users want to communicate with one another using symmetric encryption. Each of the two users is in possession of private key only known to him. For User A having the private key 6, and User B the private key 12, and a commonly known prime 71 and its primitive element 7, find the common key, and describe the procedure the two users use, to obtain this common key (i.e. draw a sequence diagram with all the messages, using the specific values given above, exchanged between the two).

Problem 19.4. We use the Diffie Hellman Key exchange with the following conditions:

Your private key and public key are X and $Y = a^X \ mod \ p$, respectively, where $p = 29$ and $a = 2$; my public key is 15.

(i) Choose your private key X and calculate your public key Y.

(ii) Calculate the common key K.

Problem 19.5. In the Diffie Hellman Key exchange protocol between user A and B both users have a private key: $X_A = 2(6)$ and $X_B = 35(12)$, respectively. The public keys are $Y_A = a^{X_A}$ *modulo* p and $Y_B = a^{X_B}$ *modulo* p. What is the common key K for $p = 71$ and $a = 7$?

Problem 19.6. We use the Diffie Hellman Key exchange with the following conditions:

A private key X and a public key $Y = a^X$ *modulo* p, where $p = 13$; the primitive element is $a = 2$; my public key is 10.

Step 1. Choose your private number X and calculate your public key $Y = 2^X$ *modulo* 13.
EXAMPLE of an answer: $X = 5$; $Y = 8$. Other answers depend on X.

Step 2. Calculate the common key $K = 10^X$ *modulo* 13. Calculate my private key.

Problem 19.7. We use the Diffie Hellman Key exchange with private keys X and Y and public keys $Z_1 = a^X$ *modulo* p and $Z_2 = a^Y$ *modulo* p, where $p = 17$ and $X = 8$.

(i) Choose a primitive element a.

(ii) Choose your private key Y , calculate your public key Z_2 and calculate the common key K.

Problem 19.8. We use the Diffie Hellman Key exchange with: private key X and public key $Y = a^X$ *modulo* p, where $p = 31$ and $a = 3$; my public key is 21.

(i) Choose your private key X and calculate your public key Y.

(ii) Calculate the common key K.

Problem 19.9. We use the Diffie Hellman key exchange with two users where $p = 11$ and $a = 8$. User A has a public key 7.

- As user B, choose a private key and calculate the public key respectively.
  $X_B = \ldots\ldots$
  $Y_B = \ldots\ldots$

- Calculate the common key.
  $K_{AB} = \ldots\ldots$

Problem 19.10. We use Diffie Hellman key exchange with two users A and B where $p = 23$.

Q1: Calculate the smallest primitive element for the given prime number, i.e. $p = 23$.

Q2: User A chooses a secret key $X_A = 5$ and user B chooses a secret key $X_B = 3$. Calculate the common key.

Q3: Does the Diffie-Hellman key exchange provide authentication of the parties? Why or why not? Give a reason.

Problem 19.11. We use the Diffie Hellman key exchange with two users.

Q_A) Calculate the largest primitive element for a given prime number p=11.

Q_B) User A chooses a secret key $X_A = 5$ and user B chooses a secret key $X_B = 3$. Calculate the common key K for the largest primitive element.

Problem 19.12. Assume that two users want to establish a common secret key over an insecure channel by using Diffie-Hellman key exchange protocol. The public key for user A is $Y_A = a^{X_A} \ mod \ p$ and for user B is $Y_B = a^{X_B} \ mod \ p$.

(Q_1) Would any of the following a and p be good choices for the Diffie-Hellman algorithm (ignoring the fact that the numbers are too small to be secure)? Motivate your answer.

$a = 1$, $p = 179$.

$a = 2$, $p = 17$.

$a = 14$, $p = 195$.

(Q_2) Describe a way to generalize the Diffie-Hellman protocol to three parties. Show the communication between the users.

Problem 19.13. The last four numbers of your matriculation number is represented as $m_4m_3m_2m_1$.

Assume that two users want to establish a common secret key over an insecure channel by using Diffie-Hellman key exchange protocol. The private key for user A is $X_A = m_3 + m_1 + 2$ and for user B is $X_B = m_4 + 7$. We consider a commonly known prime 23.

(Q1) Calculate the smallest primitive element for p = 23. (Show your steps clearly.)

(Q2) Obtain the common key by using the primitive element found above (Show your steps).

Problem 19.14. We use the Diffie Hellman Key exchange with private keys X and Y and public keys $Z_1 = a^X$ *modulo* p and $Z_2 = a^Y$ *modulo* p. We assume $p = 71$, $a = 7$.

Q1. Give two possible pairs (X, Y) such that the common key $K = 1$.

Q2. An attacker knows that the product $Z_1 * Z_2 = 7$ modulo p.
Give two possible pairs (X, Y) that satisfy the attackers knowledge.

20 Pohlig-Hellman a-symmetric Encryption

Problem 20.1. Why does the shared secret in the Pohlig-Hellman encryption have to satisfy the equation $ed = 1 \ mod \ (p-1)$?

Hint: There is a relation to primitive elements...

Problem 20.2. Two communicators in the Pohlig-Hellman a-symmetric encryption system have as a secret two numbers (e, d) such that $e.d = 1 \ modulo \ (p-1)$, where p is a prime number. The encryption rule for message M is $C = M^e \ mod \ p$.

(i) Calculate d for given $e = 15$ where $p = 53$.

(ii) What is the message that corresponds to received cipher $C = 7$? (Show your steps.)

Problem 20.3. Two communicators in the Pohlig-Hellman a-symmetric encryption system have as a secret two numbers (e, d) such that $ed = 1 \ modulo \ (p-1)$, where p is a prime number. The encryption rule for message M is $C = M^e \ mod \ p$.

(i) Give two possible numbers (e, d) for a) $p = 47$; b) $p = 43$.

(ii) What is the message that corresponds to a received cipher a) $c = 19$; b) $c = 3$?

Problem 20.4. Consider **the last 3 numbers of your matriculation number**. For the simplicity, the last 3 numbers will be denoted as $\{mat_1, mat_2, mat_3\}$. (Ex.: m.n.= 1457652, then $\{mat_1 = 6, mat_2 = 5, mat_3 = 2\}$).

Two communicators in the Pohlig-Hellman a-symmetric encryption system have as a secret two numbers (e, d) such that e.d = 1 modulo (p - 1), where p is a prime number. The encryption rule for message M is $C = M^e$ mod p.

(Q1) Calculate d for given e = 23 where p = 257.

(Q2) Explain the decryption rule and decrypt the message that corresponds to received cipher C = 16 (Show your steps.).

21 ElGamal

Problem 21.1. In ElGamal encryption, the process for decryption at user B receiving a message from a user A is given as:

Step 1) $K = C_1^{X_B} \ mod \ p$.

Step 2) $M = C_2/K \ mod \ p$ where C_1 and C_2 are the cipher texts and X_B is the private key of the receiver. The message (C_1, C_2) was composed by calculating:

$$C_1 = a^{X_A} \ mod \ p$$

$$C_2 = YB^{X_A} * M \ mod \ p$$

where Y_B is the public key of user B and a the common prime element.

(i) Explain why this encryption scheme is similar to the Diffie-Hellman key exchange.

(ii) Proof that the result of the decryption is indeed the transmitted message M.

Problem 21.2. We recall the ElGamal cryptosystem. A community of users shares a large prime p and a primitive element a. Each user has a key pair (x, Y), where $0 < x < p - 1$ is randomly chosen and $Y = a^x \ mod \ p$. Y is public and x is private.

To send a message M to Alice, who has key pair (x_A, Y_A), Bob performs the following steps:

1. Choose a random x_B with $0 < x_B < p - 1$.
2. Compute $c_1 = a^{x_B} \ mod \ p$ and $c_2 = M.YA^{x_B} \ mod \ p$.
3. The ciphertext is (c_1, c_2).

(i) Explain how Alice decrypts the message, show the steps.

(ii) Assume that prime $p = 17$ and the primitive element $a = 6$. Bob, who has a private key $x_B = 12$ wants to send a message $M = 5$ to Alice, who has a public key $Y_A = 15$. Compute the ciphertext is (c_1, c_2) and show your steps.

(iii) Alice has a private key $x_A = 10$. Show that how Alice decrypts the message.

Hint: K^{-1} should be determined such that $K^{-1}.K = 1 \ mod \ p$.

Problem 21.3. Let $(p, a, Y_B) = (53, 2, 16)$ be the public-key of an ElGamal cryptosystem and $(C_1, C_2) = (15, 50)$ be a ciphertext with this cryptosystem. What is the corresponding plaintext?

Problem 21.4. Consider **the last 3 numbers of your matriculation number**. For the simplicity, the last 3 numbers will be denoted as $\{mat_1, mat_2, mat_3\}$. (Ex.: m.n.= 1457652, then $\{mat_1 = 6, mat_2 = 5, mat_3 = 2\}$).

We recall the ElGamal cryptosystem. A community of users shares a large prime p and a primitive element a. Each user has a key pair (x, Y), where $0 < x < p - 1$ is randomly chosen and $Y = a^x$ mod p. Y is public and x is private.

(Q1) Assume that prime p = 31 and the primitive element a = 3. Bob, who has a private key $x_B = 28$ wants to send a message M = $\{mat_1 + mat_2 + mat_3\}$ to Alice, who has a public key $Y_A = 16$. Compute the ciphertext (c1, c2) and show your steps.

(Q2) Alice has a private key $x_A = 6$. Show how Alice decrypts the message.

Problem 21.5. Given $n = 71$ and $k = 7$ find k^{-1} such that $k^{-1}k = 1$ modulo 71.

22 RSA System

Problem 22.1. Why do the public key e and the private key d in the RSA encryption have to satisfy the equation $ed = 1 \ mod \ (p-1)(q-1)$?

Try to reason in formulas rather than text, it is much easier...

Problem 22.2. The RSA system was used to encrypt the message M into the cipher-text $C = 6$. The public key is given by $n = p.q = 187$ and $e = 107$. In the following, we will try to crack the system and to determine the original message M.

(i) What parameters comprises the public key and what parameters the private key?

(ii) What steps are necessary to determine the private key from the public key?

(iii) Determine the private key for the given system.

(iv) What is the original message M?

Problem 22.3. The RSA system was used to encrypt the message M into the cipher-text $C = 9$. The public key is given by $n = 143$ and $e = 23$. In the following, we will try to crack the system and to determine the original message M.

(i) What parameters comprises the public key and what parameters the private key?

(ii) What steps are necessary to determine the private key from the public key?

(iii) Determine the private key for the given system.

(iv) What is the original message M?

Problem 22.4. Assume a public key for RSA encryption given by the pair $(143, 11)$.

(i) Find the private key to the given public key.

(ii) Decode the message (111 4 88 57 116 67), assuming the letters were represented by ASCII values.

(iii) Explain why one would never use the given public key for real encryption, and what one would do to make it really secure.

Problem 22.5. Suppose that we use the RSA scheme with public key $(n = p * q, e) = (55, 7)$.

(i) Find the private key d. (For RSA we have $ed = 1$ *modulo* $(p-1)(q-1)$.)

(ii) Find the corresponding message M for a cipher $C = 3$.

Problem 22.6. For RSA, we have $n = pq = 55$; $e = 67$; $ed = 1$ *modulo* $(p-1)(q-1)$. $d = \cdots\cdots$

Problem 22.7. We want to use the RSA scheme for security.

1. We choose the integer 77 as the product of 2 prime numbers p and q.

2. For the public key d and private key e, we have the relation $ed = 1$ *modulo* $(p-1)(q-1)$.

(i) What is the public key d for a private key $e = 43$?

(ii) Give the message M for an intercepted cipher $C = 5$.

Problem 22.8. We want to be able to transmit 64 different messages.

(i) How many binary digits do we need to uniquely specify every message?

(ii) We want to use the RSA scheme for security and thus:

1. We have to choose an integer N that is the product of 2 prime numbers p and q.
2. For the private key e and public key d, we have the relation $ed = 1$ *modulo* $(p-1)(q-1)$.

Choose the best (smallest) possible $N = p \times q$ that allows independent message encryption

Problem 22.9. We want to use the RSA scheme for security.

1. We choose the integer 91 as the product of 2 prime numbers p and q.

2. For the public key d and private key e, we have the relation $ed = 1$ *modulo* $(p-1)(q-1)$.

(i) What is the public key d for a private key $e = 29$?

(ii) Give the message M for an intercepted cipher $C = 5$.

Problem 22.10. We want to be able to transmit 132 different messages.

(i) How many binary digits do we need to uniquely specify every message?

(ii) We want to use the RSA scheme for security and thus:

1. We have to choose an integer N that is the product of 2 prime numbers p and q.
2. For the private key d and public key e, we have the relation $ed = 1$ *modulo* $(p-1)(q-1)$.

   Choose the best (smallest) possible $N = p \times q$ that allows independent message encryption. Later we choose the integer 143 as the product of 2 prime numbers p and q.

(iii) What is the private key d for a public key $e = 11$?

(iv) Give the cipher for the message $M = 5$.

Problem 22.11. Local Area Network uses a public key infrastructure based on RSA, with known public number $N = p.q = 55$. User A and B have public keys 3 and 7, respectively. User C encrypts a message $M = 13$ for A and B.

(i) Calculate the encrypted messages C_A and C_B.
$C_A = 13^3 \ mod \ 55 = \ldots\ldots$
$C_B = 13^7 \ mod \ 55 = \ldots\ldots$

(ii) Calculate the corresponding private keys d_A and d_B.
$d_A = \ldots\ldots$
$d_B = \ldots\ldots$

(iii) Assume that an observer sees $C_A = 13$ and $C_B = 28$. How can he calculate the corresponding message without knowing public number N where we assume that the observer can not calculate d_A and d_B? Hint: use the fact that $gcd(3, 7) = 1$.

Problem 22.12. Given $p = 19$, $q = 29$, $N = p.q$ and $e = 17$, compute the private key d corresponding to the RSA system.

Hint: $e.d = 1\ mod\ (p-1)(q-1)$.

Problem 22.13. Consider a RSA public-key system where the public key consists of $N = pq = 143$ and $e = 71$. The encryption function is given as $C = M^e\ modulo\ N$.

Q1: Find a number d such that $ed = 1\ modulo\ (p-1)(q-1)$.

Q2: Give the decryption function for RSA.

Q3: Decrypt the cipher $C = 12$.

Problem 22.14. Given secret two large primes p and q, RSA modulus N can be computed as $N = p.q$. Answer the following questions for $N = 77 = 7 \cdot 11$.

Q_A) Which of $e = 3$ and $e = 17$ is usable as RSA public key for this N? Why or why not?

Q_B) Compute the private key d corresponding to your answer e in Q_A.

Problem 22.15. Alice has published her RSA public keys as $< N, e > = < 91, 5 >$, where N is the known public number and e is her public key. Accordingly, Bob sent her the cipher text 81.

Find the corresponding message.

Problem 22.16. Consider **the last 3 numbers of your matriculation number**. For the simplicity, the last 3 numbers will be denoted as $\{mat_1, mat_2, mat_3\}$. (Ex.: m.n.= 1457652, then $\{mat_1 = 6, mat_2 = 5, mat_3 = 2\}$).

The cipher $(mat_1 + 33 + mat_3)$ was obtained from the RSA algorithm using $n = 11413$ and $e = 7467$.

Using the factorization $11413 = 101.113$, find the plaintext.

23 Euclid's algorithm

Problem 23.1. We recall the Euclid's algorithm. Let e and p be two integers with $gcd(e, p) = 1$. Then there exist two integers d and n such that $e.d+n.p = 1$ where d is called the inverse of e modulo p, since $e.d = 1$ *modulo* p.

Let us look at an example:

Suppose that $e = 107$. The inverse of $e = 107$ *modulo* 160 can be calculated as follows:

$160 = 107.1 + 53 \quad gcd(160, 107) = gcd(107, 53)$

$107 = 53.2 + 1 \quad gcd(107, 53) = gcd(53, 1) = 1$

From above, we can conclude that there exist two integers d and n such that $e.d + n.p = 1$. In order to form $e.d + n.p = 1$, we need to reshape the second equation:

$1 = 107 - 53.2$

Replace 53 with the first equation:

$1 = 107 - 53.2$

$1 = 107 - (160 - 107).2$

$1 = 3.107 - 2.160$

So we can see that $d = 3$. General formula is given in script.

Find the inverse element of $e = 17$ *modulo* 2882.

Problem 23.2. Calculate the greatest common divisor of 14212 and 248.

Problem 23.3. Calculate the greatest common divisor of 6564 and 532 .

Problem 23.4. Calculate the greatest common divisor of 10434 and 522.

Problem 23.5. Consider **the last 3 numbers of your matriculation number**. For the simplicity, the last 3 numbers will be denoted as $\{mat_1, mat_2, mat_3\}$. (Ex.: m.n.= 1457652, then $\{mat_1 = 6, mat_2 = 5, mat_3 = 2\}$).

Find the inverse of $(mat_1 mat_2 mat_3)$ mod 1009? (Ex.: m.n.= 1457652, then $(mat_1 mat_2 mat_3)$=652).

Problem 23.6. (Q1) Find integers x and y such that $17x + 101y = 1$.

(Q2) Find d such that $7d \equiv 1$ $(mod$ 101).

24 Protocol Failure

Problem 24.1. In this problem, we investigate a failure in RSA system. We assume two users A and B with public keys $P_A = (n, e_1)$ and $P_B = (n, e_2)$ where n is the modulus and e_1 and e_2 are the chosen public key encryption exponents. (e_1 and e_2 are relatively prime, i.e. $gcd(e_1, e_2) = 1$.) A third user, Alice, sends the same message x to both. An attacker Oscar intercepts y and z which can be calculated as $y = x^{e_1} \ mod \ n$ and $z = x^{e_2} \ mod \ n$. Oscar then computes $c_1 = e_1^{-1} \ mod \ e_2$ and $c_2 = (c_1 e_1 - 1)/e_2$. (Note that c_2 is an integer since $c_1 e_1 = 1 \ mod \ e_2$.) Finally, Oscar computes $y^{c_1}(z^{c_2})^{-1} \ mod \ n$.

(i) Prove that the last value Oscar computes is x. Thus, Oscar can decrypt the message Alice sent, even though the cryptosystem may be secure.

(ii) Illustrate the attack by computing x by this method if $n = 18721$, $e_1 = 43$, $e_2 = 7717$, $y = 12667$ and $z = 14702$. In this case, compute c_1 by using Euclid's Algorithm. Hint: you don't need to simplify x.

25 Complexity

Problem 25.1. For the following program, compute the time complexity as a function of n. "Loop body" can be assumed as a constant number of lines of code. Briefly explain how you obtained your result.

Hint: Try to write a generalized equation to express the number of times the loop body is executed.

for $(i = 0,\ i <= n - 1;\ i + +)$ {
for $(j = i + 1;\ j <= n - 1,\ j + +)$ {
loop body
}
}

Problem 25.2. Assume one wants to calculate $a^n \ mod\ p$.

(i) Describe an algorithm in pseudo-code to calculate $a^n \ mod\ p$ for fixed n.

(ii) What is the complexity of your algorithm in terms of n?

(iii) Assume that n is chosen randomly with $0 < n < p$. What is the complexity of your algorithm now in terms of p?

26 Authentication

Problem 26.1. Give a brief definition of the terms below:

(i) Zero knowledge protocol,

(ii) Authentication,

(iii) Man in the middle attack.

Problem 26.2. Alice and Bob have a shared secret k and have decided to use it in the following protocol, which enables Alice to identify Bob as the party at the other end.

1. Alice picks a random string r and sends it as challenge to Bob.
2. Bob responds with $r \oplus k$.

Alice's and Bob's analysis of the protocol is this: The protocol does indeed provide identification, since Alice can check that the sender of message 2 knows k. It is also secure, since only random numbers are ever sent on the communication channel.

(i) How does Alice check that the sender of message 2 knows k?
(ii) Do you agree with Alice and Bob about the security of their protocol? Motivate your answer!

Problem 26.3. Consider the following authentication protocol, which is used in a classical cryptosystem. Alice generates a random message r, enciphers it with the key K which is shared with Bob. She sends the encrypted message to Bob. Bob deciphers it and computes $r + 1$. He encrypts this message again with key K and sends the resulting ciphertext back to Alice. Alice deciphers the message and compares it with r. If the difference is 1, she knows that her correspondent shares the same key K and is therefore Bob. If not, she assumes that her correspondent does not share the key K and so is not Bob.

(i) Write down the protocol in the mathematical notion like in lecture notes.

(ii) Does this protocol authenticate Bob to Alice? Why or why not?

Hint: Protocol does not provide any possibility to store the already used random numbers. Try to think a possible attack.

Problem 26.4. An organization uses a public key encryption scheme E where each user has a key pair (e, d). Here e is the public encryption key and d is the private decryption key. Further, the organization has devised the following protocol, where each receiver acknowledges receipt of the message:

$$\begin{array}{lrcl} 1. & A \to B & : & A, B, E_{eB}(m). \\ 2. & B \to A & : & B, A, E_{eA}(m). \end{array}$$

A wants to send message m to B and therefore sends a message containing the names of the two parties and the message encrypted for B. B acknowledges the message by first decrypting the last part to recover m and then sending back a similarly structured message to A, but with the roles of the two parties interchanged. A can now decrypt the last part, check that she gets m and conclude that B has indeed receiverd m.

(i) This protocol is not secure against adversaries within the organization. More precisely, consider an adversary who himself has a key pair and can send messages and get them acknowledged. Show that if he, by eavesdropping, gets access to the two messages sent in the protocol run between A and B, he can go on to recover m.

(ii) Both messages in the protocol have the structure S, R, $E_{eR}(m)$, where S denotes Sender and R denotes Receiver of the message. It is proposed to modify the message structure to S, R, $E_{eR}(m||X)$ for some suitable X, where $m||X$ denotes the concatenation of m and X. For each of the following three proposals for X, explain why or why not it prevents the attack from (i).

1. $X = S$.
2. $X = R$.
3. X = message number within the run, i.e. $X = 1$ for the first message and $X = 2$ for the second.

Problem 26.5. Smart Cards store some information used for authentication and encryption of connections.

(i) Give a list of possible items which could be stored on a smart card.

(ii) How are those items secured on the smart card?

(iii) What is an additional benefit of smart cards, other than being able to store information?

27 Protocols

Problem 27.1. Alice and Bob have invented the following protocol for sending a message securely from A to B. The protocol is based on the ideas of the one-time pad, but without a common, shared secret. Instead, for each message, both A and B invent a random nonce and execute the following protocol to send message M from A to B

1. $A \longrightarrow B : M1 = M \oplus N_A$
2. $B \longrightarrow A : M2 = M1 \oplus N_B$
3. $A \longrightarrow B : M2 \oplus N_A$

Here, in 3 turns only the messages $M1$, $M2$ and $M2 \oplus N_A$ in the right hand side are sent.

(Q_1) Show that B can recover M.

(Q_2) Is the system secure? Why or why not?

Problem 27.2. Given is a protocol in which the sender performs the following operation.

$$\text{Protocol: } Y = E[(M||H(M)), K]$$

where M is the message, H is a hash function, E is an encryption algorithm, $'||'$ denotes simple concatenation, and K is the secret key which is only known to the sender and the receiver. Assume that the sender and the receiver know concatenation and deconcatenation structure.
Q) Provide a step-by-step description (e.g., with an itemized list) of what the receiver does upon reception of Y.

Problem 27.3. We recall the CBC mode of encryption of a message $M = M_1M_2M_3...M_n$, where M_i is block number i of M. Then the encrypted message is $C_0C_1C_2...C_n$, where

$$C_0 = IV \tag{3}$$
$$C_i = E_K(M_i \oplus C_{i-1}), i = 1, 2, ...n. \tag{4}$$

IV stands for the initialization vector. Now we consider the following beginning of a protocol:

$$A \rightarrow B : N_A \tag{5}$$
$$B \rightarrow A : \{N_A, K\}_{K_{AB}} \tag{6}$$

We do not need to know more about the protocol (which may contain further messages) than the following:

- A and B share a long-term AES key K_{AB}; the notation $\{\star\}_{K_{AB}}$ denotes encryption of $\star$ using AES in CBC mode (block size 128 bits).
- N_A is a 128 bit nonce chosen by A and K is a 128 bit session key chosen by B.

In the second message, B includes N_A to ensure freshness and K as a session key for the session just started. When A receives the second message, she thus concludes that B is alive at the other end and has just chosen a fresh session key K.
Now consider the following scenario: The adversary C eavesdrops on a run of this protocol between A and B and stores messages sent. Because of an unspecified mistake by A or B (outside the protocol), C gets hold of K and can of course read all subsequent messages in the session. But, the situation is worse than that, as we shall see.
Let message 2 in the run described above be $C_0C_1C_2$ (three blocks; the IV and two encrypted blocks). The next day, A and B initiate a new session. C again eavesdrops and now intercepts the second message $C_0'C_1'C_2'$, changes it to $C_0'C_1'C2$ and sends the changed message to A, pretending to be B. Show that A will accept the message as the reply to her first message in the new run and that C will know the session key of the new run and thus can continue the session with A, pretending to be B. Explain your result.

28 Hash Functions

Problem 28.1. For the following scenarios, give recommendations for what cryptographic measures are required to achieve the intended goal(s):

(i) In a distributed computation system on the Internet (such as e.g. SETI@home) one wants to assure that values transmitted over the Internet are not modified between the main site and the computation nodes.

(ii) Most banks these days allow money transfer being done over the Internet. For a transfer order, the bank of course wants to be sure, that it is really the owner of the bank account who gives the order of the money transfer.

(iii) A company doing research would like to exchange information in a secure way among their different locations.

Problem 28.2. We consider cryptographic hash functions.

(a) Give a brief definition of hash functions.

(b) What are the two basic attacks against a hash function? Explain them briefly and stress the differences.

(c) Give an interpretation of the term collision resistance.

(d) Assume that for a given message X, a hash function produces a 5-bit output.

1. How many experiments on the average would one require in order to find a message X' that gives the same hash value, i.e. $Hash(X) = Hash(X')$?

2. How many random messages would one require such that the probability of finding at least one X' is larger than $1/2$ where $Hash(X) = Hash(X')$?

(e) We still consider a hash function which produces a 5-bit output. How many random messages would one require such that the probability of finding two messages (Z, Z') is larger than $1/2$ where $Hash(Z) = Hash(Z')$?

Problem 28.3. We consider cryptographic hash functions.

(a) Give a brief definition of hash functions.

(b) What are the two basic attacks against a hash function? Explain them briefly and stress the differences.

(c) Give an interpretation of the term collision resistance.

(d) Assume that for a given message X, a hash function produces a 6-bit output.

1. How many random messages would one require in order to find a message X' that gives the same hash value, i.e. $Hash(X) = Hash(X')$?

2. How many random messages would one require such that the probability of finding at least one X' is larger than $3/4$ where $Hash(X) = Hash(X')$?

(e) We still consider a hash function which produces a 6-bit output.

1. How many random messages would one require in order to find two messages (Z, Z') that give the same hash value, i.e. $Hash(Z) = Hash(Z')$?

2. How many random messages would one require such that the probability of finding two messages (Z, Z') is larger than $3/4$ where $Hash(Z) = Hash(Z')$?

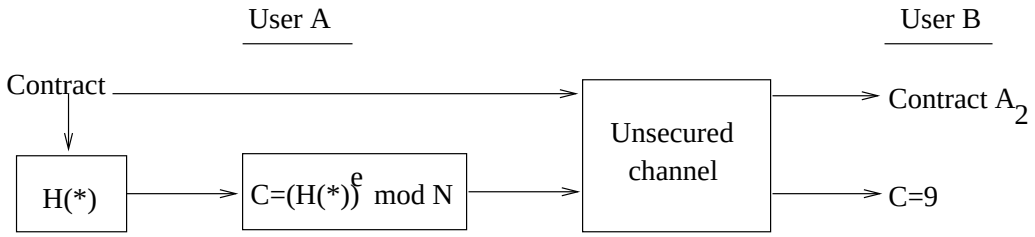
Problem 28.4. Explain why transmitting a hash value of a password instead of a plain text password, when only the hash value of a password is stored on the host, does not solve any of the problems of plain text passwords.

Give at least one possible attack on such hashed passwords.

Problem 28.5. Consider the following system where user A wants to send a contract to user B. Figure 43 illustrates the transmission.

User A sends the encrypted hash function of the contract as well as the contract itself. After transmission over an unsecured channel, user B receives a contract "A_2" and a cipher $C = 9$. We consider a hash function, which maps the input data to its output according to the following lookup table. (ex: $H(Contract = A_1) = 4$.)

Figure 43:



Contract	$H(*)$
A_1	4
A_2	56
A_3	81

(i) Why do we need to use a hash function? Explain briefly.

(ii) Let the encryption scheme given in the system satisfy the requirements of the RSA algorithm. Given $N = p.q = 91$ and the encryption key $e = 59$, find the decryption key d such that $e.d = 1 \ mod \ (p-1)(q-1)$. ($d$ =?)

(iii) Calculate the related message of the received cipher and check whether the contract is the original one or just an alteration. Show your steps clearly!

Problem 28.6. Given is a protocol in which the sender performs the following operation:

$$y = e[(M||H(k_2||M)), k_1]$$

where M is the message, H is a hash function, e is an encryption algorithm, $'||'$ denotes simple concatenation, and k_1, k_2 are secret keys which are only known to the sender and the receiver. Assume that the sender and the receiver knows concatenation and deconcatenation structure.

(i) Provide a step-by-step description (e.g., with an itemized list) of what the receiver does upon reception of y.

(ii) For the following questions, the statement is either correct or wrong. Circle yes or no.

1. An attacker can alter the Message M. (YES / NO)
2. Given protocol does not provide authentication. (YES / NO)
3. Signature can not be repudiated. (YES / NO)

Problem 28.7. Show all your steps.

a) If there are 30 people in a classroom, what is the probability that at least two have the same birthday?

b) How many people should there be in a classroom in order to have 100 percentage probability that at least two have the same birthday?

Problem 28.8. A hash function H should have the following properties to be useful for the message authentication.

a) H can be applied to a block of data of any size.

b) H produces a fixed-length output.

c) $H(x)$ should be relatively easy to compute.

d) For any given value h, it is computationally infeasible to find x such that $H(x) = h$.

e) For any given block x, it is computationally infeasible to find $x \neq y$ such that $H(x) = H(y)$.

f) It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.

Consider the following hash function. Messages are in the form of a sequence of decimal numbers, $M = (a_1, a_2, \ldots, a_t)$. The hash value h is calculated as $(\sum_{i=1}^{t} a_i)\ mod\ n$, for some predefined value n.

Q_1) Calculate the hash function for $M = (189, 632, 900, 722, 349)$ and n=989.

Q_2) Does this function satisfy any of the requirements for a hash function listed above. Explain your answer in general.

Problem 28.9. Consider the following proposed signature scheme. The setting is for a large prime p and a primitive element a. A user has a private key x and a public key $X = a^x \bmod p$. To sign message m, one first computes $h = H(m)$ for some hash function H. Then one computes $z = (x/h) \bmod p$ (we require $h \neq 0$). The signature is $a^z \bmod p$. Verification of signature namely s consists of checking that $s^h = X \bmod p$. Is this a good scheme, i.e.

(Q_1) will correct signatures be accepted?

(Q_2) is it infeasible to sign an arbitrary message without knowing x?

29 Cipher Modes

Problem 29.1. We consider block cipher modes which encrypt a plaintext $M_1M_2...M_n$ to produce a ciphertext $C_0C_1C_2...C_n$ using a random nonce N.

a) The mode CBC using the recurrence

$C_0 = N$
$C_i = E_K(M_i \oplus C_{i-1}),\ i = 1, 2, ...$

How is decryption performed? (Note that here, as in all your answers, you must give motivations that show that your answer is correct!)

b) Counter mode instead uses the equations

$K_i = E_K(N||i), i = 1, 2..$

$C_0 = N$

$C_i = M_i \oplus K_i, i = 1, 2...$

In this mode, $||$ represents the concatenation. How is decryption performed?

c) Consider the following proposal for a block cipher mode:

$C_0 = N$

$C_i = E_K(M_i) \oplus C_{i-1},\ i = 1, 2...$

This is not a useful mode; why?

30 Pseudo Random Number Generators

Problem 30.1. We construct a pseudo random number generator as follows:

$$\begin{aligned} C_0 = 1, \text{ for } i > 0 & \\ \text{calculate } C_i &= C_{i-1} * P \text{ modulo } 17 \\ R_i &= C_i \text{ modulo } 2. \end{aligned}$$

Q1) Determine R_1, R_2, R_3, ...,R_{17} (17 values) for $P = 2$ and for $P = 3$.

Q2) Which P is better? Why?

31 Linear Feedback Shift Register

Problem 31.1. The output sequence of a random number generator with 4 register is given as (10111001) where rightmost bit is first in the sequence.

- Write down the seed of the register at time instance 0 (starting point).
- Give the mathematical relation by constructing the C, X_1 and X_2 matrices.
- Find the connections c of the shift register.
- Draw the diagram for the shift register.
- What is the period of this shift register. Is this the maximum period?
- Implement the same output sequence of a random generator with 3 register. (Draw the diagram!) Is this the maximum period of this register?

Problem 31.2. The output sequence of a random number generator with 3 register is given as (001110) where rightmost bit represents the first output in the sequence.

- Write down the seed of the register at time instance 0 (starting point).
- Give the mathematical relation by constructing the C, X_1 and X_2 matrices.
- Find the connections c of the shift register.
- Draw the diagram for the shift register.
- What is the period of this shift register? Write down the complete period sequence. Is this the maximum period?
- Show how the plaintext (110001100101100010001011) is encrypted by a stream cipher that uses this LFSR as key generator?

Problem 31.3. Consider a Linear Feedback Shift Register (LFSR) defined by the sequence $c = (1, 0, 0, 1)$.

- Draw the diagram for this shift register.

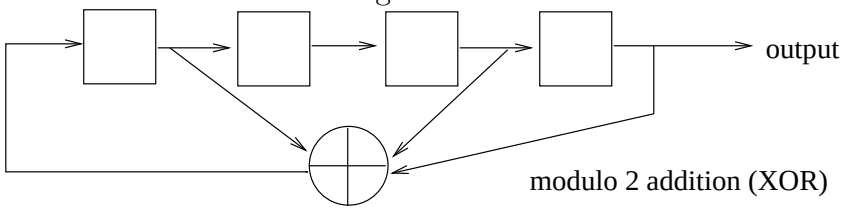
- When the seed is 0101 (Leftmost register first!), what is the output sequence of the shift register?
- What is the period of this shift register?
- Is this a good random number generator, if one expects $P(0) = P(1) = 0.5$?

Problem 31.4. You observe the ouput sequence 00101001010 (rightmost bit is first in the sequence) from a random number generator based on a linear feedback shift register with 4 registers.

- What was the seed of the shift register, considering that the sequence above starts at time 0?
- Find the connections c of the shift register.

Problem 31.5. The Linear Feedback Shift Register in figure 44 has 4 memory elements:

Figure 44:



From the output sequence we know $\cdots, x_{t+3}, x_{t+2}, x_{t+1}, x_t, \cdots = \cdots, 1, 0, 1, 1, \cdots$.

(i) Give x_{t+4} and x_{t-1}.

(ii) What is the period T of the output sequence?

(iii) What is the maximum period T_{max} of this generator?

Problem 31.6. Given the sequence

....10011010111100010011.....

$time \rightarrow t$

(i) What is the minimum length of a shift register that can generate the sequence above? Why?

(ii) Draw the diagram of the Linear Feedback Shift Register that generates the given sequence above.

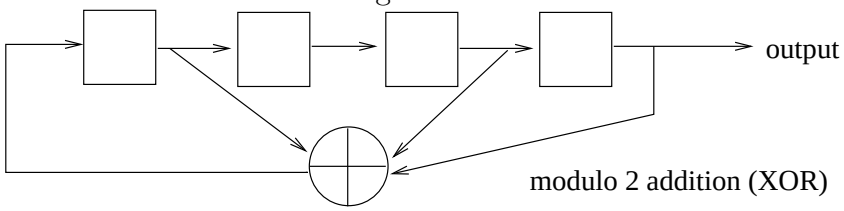
Problem 31.7. A linear feedback shift register (LFSR) generates a sequence from which we observe the following 50 bits:

...00100001111101010011000100001111101010011000100001...

Construct an LFSR of minimal length that produces this output. Show your steps clearly.

Problem 31.8. Consider the Linear Feedback Shift Register in figure 45:

Figure 45:



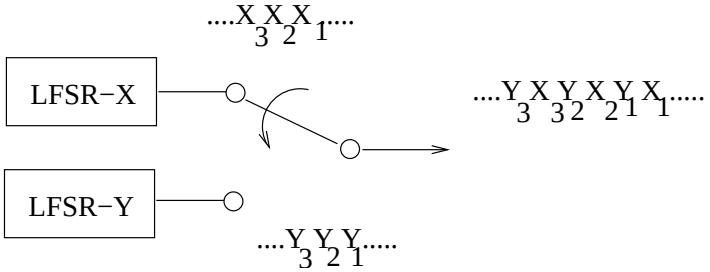
- When the seed is 0110, what is the output of the shift register? (At least 8 outputs.)
- What is the period of the given shift register?
- Is this the maximum period in the case of 4 registers? Why or why not?
- Draw a Linear Feedback Shift Register of lenght 3 that generates the same output.

Problem 31.9. Consider the Linear Feedback Shift Registers (LFSR) in figure 46 where D represents the delay elements.

Q1: For an initial content (seed) of 1,0 for both LFSR's, give the periods of the output sequences.

Figure 46:

Figure 47:



Q2: Generate a new "pseudo-random" sequence by interleaving the 2 output sequences in figure 47.

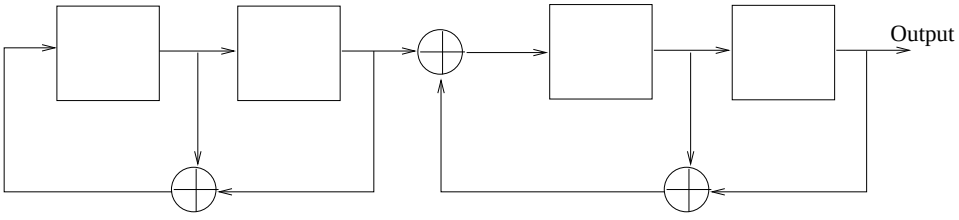
Q3: Give 16 digits of the new output sequence.

Q4: What is the period of the new sequence?

Q5: Is it possible to generate the new sequence with a LFSR of length 3? Why or why not?

Problem 31.10. We consider the cascade of two linear feedback shift registers as a pseudo random number generator as shown in figure 48.

Figure 48:

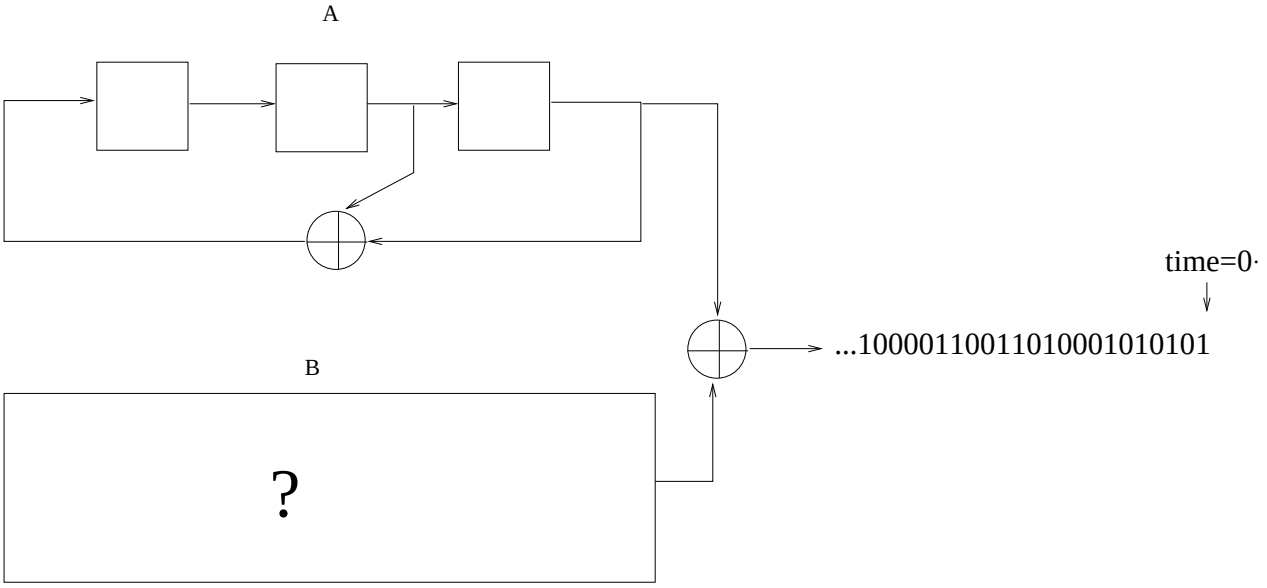


(Q_1) What is the maximum period of the output sequence?

(Q_2) Generate the output sequence of 15 bits for the initialization values of delay elements equal to 1.

Problem 31.11. We consider two linear feedback shift registers which combine their outputs using XOR as shown in figure 49. The upper LFSR is marked as A and the other LFSR as B, respectively. Let the initialization values of LFSR A be 101.

Figure 49:



(Q_1) For a given upper LFSR , design the second LFSR B such that the **given output is satisfied.**

(Q_2) Find the period of each LFSR and the output sequence.

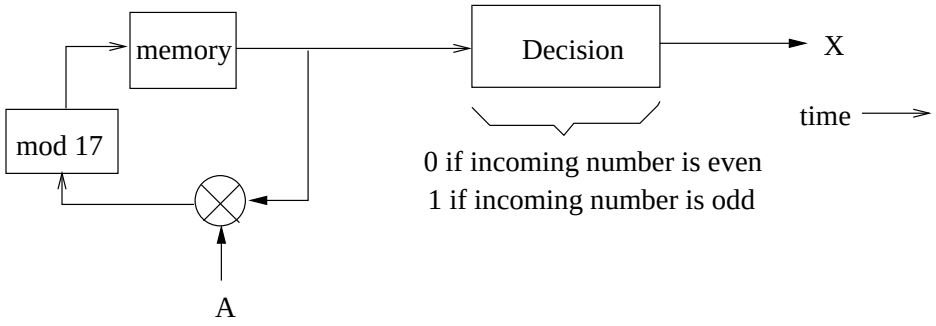
T_A =.....

T_B =.....

T_{output} = ...

Problem 31.12. Suppose that we choose a primitive element A for $p = 17$. We use A to generate a pseudo random sequence X according to the structure given in figure 50. At the beginning, the memory is initialized as A. In other words, the first input to the decision stage is A. Answer the following questions:

Figure 50:



(Q_1) Choose a primitive element A for $p = 17$.

(Q_2) Generate the sequence X using your choice A. (At least 20 outputs.)

(Q_3) What is the period of the generated sequence?

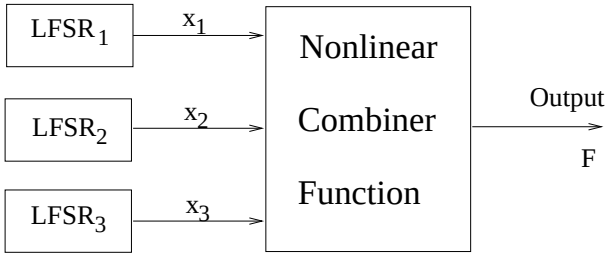
(Q_4) What is the minimum length of a shift register that can generate the sequence above? Why?

Problem 31.13. Consider the last six digits of your matriculation number. Replace each zero with **five** and convert each digit into 4-bit binary representation (ex : 2223009 $\rightarrow$ 223559 $\rightarrow$ 001000100011...). Figure 51 shows the combination of three linear feedback shift registers (LFSR) to generate a pseudo random sequence F.

Divide the sequence of 24 binary digits obtained above into 3 blocks of 8 bits (block 1=first 8 bits,...).

(Q_1) Construct three LFSR's of **minimal length** that can produce these observed blocks. The first block is an output of the first LFSR , the second block is from the second LFSR , and the third block is from the third LFSR. Assume that rightmost bit is first in the sequence and the

Figure 51:



observed blocks can be a part of any sequence. What are the seeds of the shift registers? What is the maximum period of the constructed combination generator?

(Q_2) The output can be defined as the following Boolean equations (+=OR, $\cdot$=AND,$\oplus$=XOR), where x_1, x_2 and x_3 represent the outputs from the first LFSR, the second LFSR and the third LFSR, respectively.

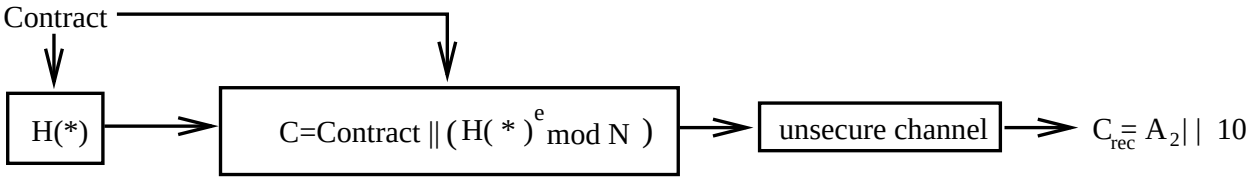
1. $F = x_1 \oplus x_2 \oplus x_3$
2. $F = x_1 \cdot x_2 \cdot x_3$
3. $F = x_1 \oplus (x_2 + x_3)$
4. $F = (x_1 \cdot x_2) \oplus (x_2 \cdot x_3) \oplus x_3$

Write down the first 20 outputs of F for each equation. Is there any correlation between F and the output of the LFSR's, namely x_1, x_2 and x_3? Give reasons.

32 Challenge Response

Problem 32.1. Consider the system in figure 52 where user A wants to send a contract to user B. The figure below illustrates the transmission.

Figure 52:



The cipher C is the concatenation of the encrypted hash function of the contract and the contract itself. We assume that the receiver knows the concatenation and the deconcatenation scheme. After transmission over an unsecured channel, receiver gets $C_{rec} = A_2||10$. We consider a hash function, which maps the input data to its output according to the following lookup table. (ex: H(Contract=A2)=12)

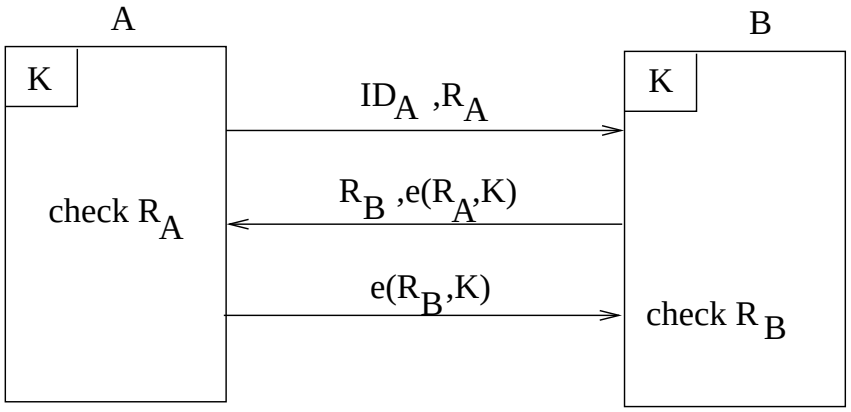
Contract	$H(*)$
A_1	6
A_2	12
A_3	9

Q1) Let the encryption scheme given in the system satisfy the requirements of the RSA algorithm. Given N=p.q=91 and the encryption key e=47, find the decryption key d such that e.d = 1 mod (p-1)(q-1). (d=?)

Q2) Check whether the contract is the original one or just an alteration. Show your steps clearly!

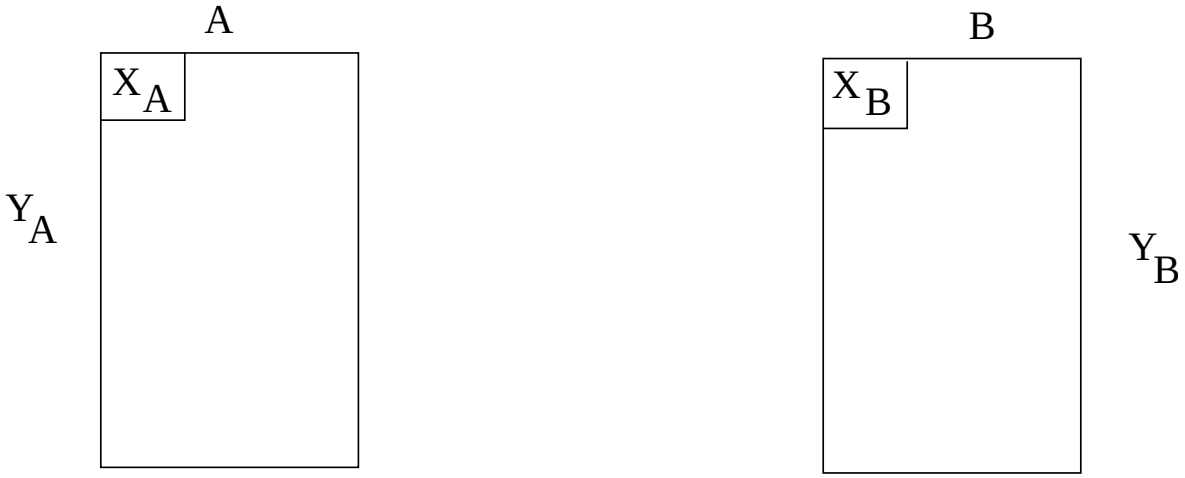
Problem 32.2. Alice and Bob are two users who want to authenticate each other. With symmetric key system, the authentication process is given in figure 53. R_A and R_B represent the random numbers, K represents the secret key, e is the encryption function and ID_A denotes identity of A.

Figure 53:



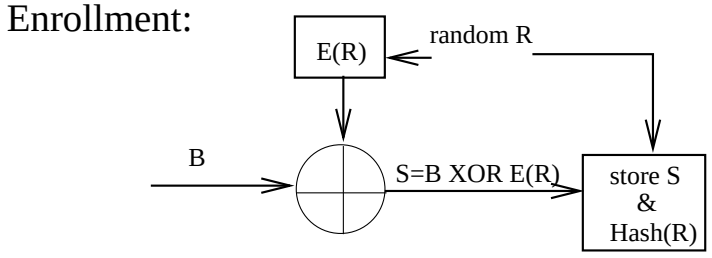
(Q) We consider public key encryption system where each of them has a private and public keys: Alice has a private key X_A and a public key Y_A, and respectively Bob has X_B and Y_B. Determine and draw a simple protocol on figure 54 which authenticates Alice and Bob to each other.

Figure 54:



33 Application of error correcting codes in biometric authentication

Problem 33.1. Let us consider the authentication system based on biometric information. The enrollment scheme is given in the figure below. In the enrollment of the fingerprint, a binary input vector B is XORed with the randomly chosen Hamming code $E(R)$. The result S and $H(R)$ (the hash value of R) are stored in the database. $E(R)$, B and R are deleted.



(Q_1) In the biometric authentication, having received an observation binary vector B' and using the content of the database, the system has to decide whether the observation vector can be considered as the corrupted version of the claimed fingerprint B or not, where the measure of closeness is the number of bit positions for which the corresponding vectors are different. Then, the authentication system has to accept or reject the claim. **Provide a step-by-step description of the authentication process.**

(Q_2) The attacker has an access to the database and discovers S and $H(R)$. Is the system still secure? Comment on the security. (H is a one way Hash function.)

(Q_3) For a given Hamming code generator matrix G below, how many possible codewords can be constructed? Write down all possible codewords $E(R)$ by showing the related vector R.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \tag{7}$$

(Q_4) What is the minimum number of bit errors that can be corrected with the code obtained in Q_3?

(Q_5) Choose B as the binary 7-bit representation of the last two digits of your matriculation number. Provide a step-by-step description of the enrollment process by randomly choosing R. Show all calculated outputs. Assume that the hash function H is collision-free (it is not the case for a short length) and the output can be simply represented as $H(*)$, where $*$ is the input bit vector.

(Q_6) In the authentication process, your fingerprint is measured as $B' = B \oplus N$, where N represents the error vector of length 7 in the measurement. Assume the error vector is given as $N = (0001000)$. Provide a step-by-step description of the authentication process and show whether the system accepts you.

(Q_7) Repeat the question Q_6 with the error vector as $N = 1000010$.

34 General Problems

- Any encryption function has to be injective. (yes/no)
- Explain in your own words why any encryption function has to be injective or not.
- In a symmetric-key cryptography, the key must remain secret at both ends. (yes/no)
- A one-way function is hard to calculate but easy to invert. (yes/no)
- In a public-key cryptography, the encryption key K_i need not be kept secret, it may be made public. (yes/no)
- The inverse of a one-way function is easy to calculate. (yes/no)
- Public key systems use one secret key for both encryption and decryption. (yes/no)
- A challenge response system cannot be used with a public key system. (yes/no)
- A digital signature is made with a public encryption key. (yes/no)
- A challenge response system can only be used with a public key system. (yes/no)
- The ENIGMA cipher is a transposition cipher. (yes/no)
- A digital signature is made with a secret encryption key. (yes/no)
- For binary words of length 3, the number of different transposition ciphers is larger than the number of substitution ciphers. (yes/no)
- What is the difference between a stream- and a block-cipher? How can one make this difference disappear?
- What makes encryption methods like RSA secure? Or in other words, where lies the difficulty in breaking RSA?
- Why do all the encryption methods require p to be prime when doing calculations modulo p?

- Using the Euclidean algorithm, find the greatest common divisor of 2002 and 2940.
- Find integers d and n such that $2002d + 2940n = gcd(2002, 2940)$.
- In theoretical security we assume that the analyst has limited resources. (yes/no)
- A plaintext attack is less powerful than a ciphertext only attack. (yes/no)
- In a network, link encryption is better than end-to-end encryption. (yes/no)
- Give 4 desirable properties of digital signatures.
- Calculate the greatest common divisor for a and b where a is the last three digits of your matriculation number and b is the second to last three digits of your matriculation number. Find e and d such that $ae + bd = gcd(a, b)$.
- Connect the items on the left with items on the right which belong to each other. Multiple connections for one item are possible:

	Keyless
Pohlig-Hellman	Secret Key Algorithm
RSA	Factorization
Hash	Block Cipher
Diffie-Hellman	Discrete Logarithm

- Draw the basic block diagram of the classical cryptosystem.
- Suppose that the last 3 digits of your matriculation number represents the number of messages. If the third right digit is zero, then consider it as 1. (Ex.: m.n.= 1457002, then the number of messages: 102).

  (Q1) How many binary digits do you need to uniquely specify every message?

  Suppose that the last 2 digits of your matriculation number represents the number of nodes in a network. If the second right digit is zero, then consider it as 1.(Ex.: m.n.= 3457602, then the number of nodes: 12).

(Q2) How many different keys do we have to generate such that every pair of nodes can communicate in a bi-directional secure way using classical cryptosystem?

(Q3) We replace classical system with a public key system. How many different keys do we have to generate such that every pair of nodes can communicate in a bi-directional secure way?