

# EXAM: Introduction to Cryptography 2I1502

23<sup>rd</sup> August 2005

You are allowed to use pen, paper, calculator (non alphanumeric) and a dictionary (English – Your Home language). You may answer the questions either in English or Swedish.

The exam consists of 70 points. You need 35 points to pass the exam.

When calculating values you might get results like  $x^y \bmod z$ , which your calculator cannot compute. It is acceptable to answer in this form.

## ***Theoretical Part***

The theoretical part consists of 7 questions together giving 35 points. Motivate your answers.

### **1. Classic Cryptography [6]**

**Question A:** The Hagelin M-209 machine had drums with teeth on them and encryption wheels with pins that could be in either active or passive mode. Describe the purpose of the teeth and the pins. (2p)

**Question B:** The Enigma machine had a plugboard into which cords were set. Describe how the cords affected the encryption process of Enigma. (2p)

**Question C:** Why is a Caesar substitution cipher in general easier to break than a reciprocal substitution cipher? (2p)

### **2. Information Theory [4]**

**Question A:** Why is the source entropy higher when generation of a sequence of letters is based on the probability distribution of monograph statistics as compared to probability distribution based on digraph statistics? (2p)

**Question B:** Rank the probability distributions below from the one with the highest uncertainty to the one with the lowest: You do not need to make a calculation (2p)

- $p(A) = 0.9, p(B) = 0.1$
- $p(A) = 0.5, p(B) = 0.5$
- $p(A) = 0.2, p(B) = 0.8$
- $p(A) = 0.0, p(B) = 1.0$ .

### 3. Stream ciphers [6]

**Question A:** A linear feedback shift register of  $n$  registers is used to create a key stream. Suppose an attacker knows the feedback function. How many values of the key stream must the attacker know to be able to calculate a future value in the key stream? Explain why. (2p)

**Question B:** A system is using three linear feedback shift registers, here denoted A, B and C. None of the generators are biased. The output of these three shift registers are combined to a key stream by using the function XOR. Discuss whether this key stream will be biased or not, and give a proof either for it being biased or for it not being biased. (2p)

**Question C:** The linear complexity of the three shift registers in question B are denoted as  $C_A$ ,  $C_B$  respectively  $C_C$ . What is the linear complexity of the created key stream? (2p)

### 4. Randomness [4]

**Question A:** Several statistical tests takes parts of for instance a key stream and puts them into categories comparing the occurrences in each category with what is expected using a  $\chi^2$  (chisquare) test. Describe one of these tests that can be used to see whether a sequence has random properties. (2p)

**Question B:** Why has a  $\chi^2$  test with  $n$  categories,  $n-1$  degrees of freedom? Describe what degrees of freedom means. (2p)

### 5. Symmetric block ciphers [6]

**Question A:** Describe in detail how CBC (Cipher Block Chaining) works. (4p)

**Question B:** What is needed for an attacker to be able to carry out a differential cryptanalysis on DES? (2p)

### 6. Asymmetric block ciphers [4]

The SSL function uses asymmetric encryption when the users exchange a session key in the beginning of the protocol. After this phase symmetric encryption is used to encrypt the traffic, for instance 3DES.

**Question A:** Why is asymmetric encryption and not symmetric encryption used to decide the session key? (2p)

**Question B:** Why is symmetric encryption and not asymmetric encryption used to encrypt the traffic after the initial phase, i.e. why is the session key symmetric? (2p)

## 7. Crypto Hacking [5]

**Question A:** Some certificates are protected with hashed passwords. To be able to use the certificate the password that results in the correct hash value must be given. Describe how an attack is carried out against a stolen certificate. (3p)

**Question B:** Later certificate standards have increased the number of iterations of hashing the password. What would be the reason to increase the value from for instance 25 iterations to 2000 iterations? (2p).

### Problems Part

The problem part consists of 7 questions with a total of 35 points. Explain your results and show your calculations. Only giving an answer will not result in any points.

#### 8. Classic Cryptography - Encryption [6]

**Question A:** You are sending a secret message to a friend of yours and want to encrypt it. You have earlier agreed on using a permutation cipher with a 6-number key being {3, 5, 2, 4, 6, 1}. How would you encrypt the text below using a permutation cipher?

*Hi, I have the piece; meet me at the usual place.*

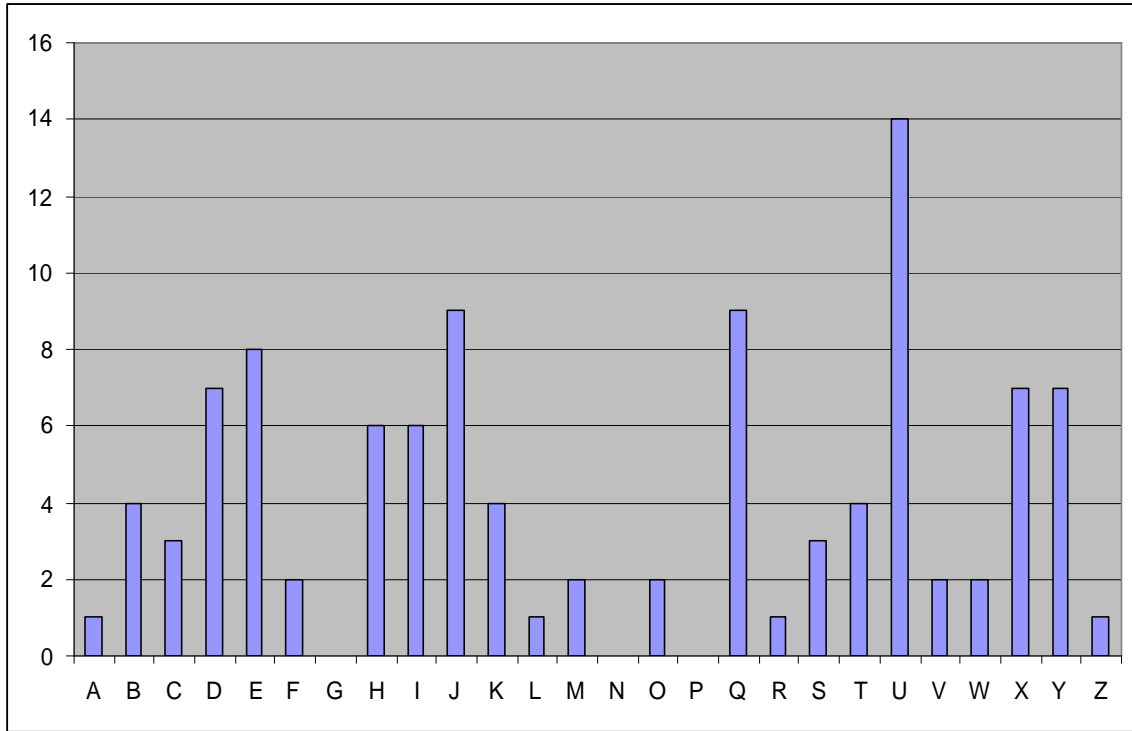
Several different answers are possible and will be accepted. (3p)

**Question B:** Route transposition has sometimes been used to make it easier to remember a longer key. Below a 5 \* 5 matrix is shown. Create your own key and encrypt the following message: *The money will arrive today.* (3p)

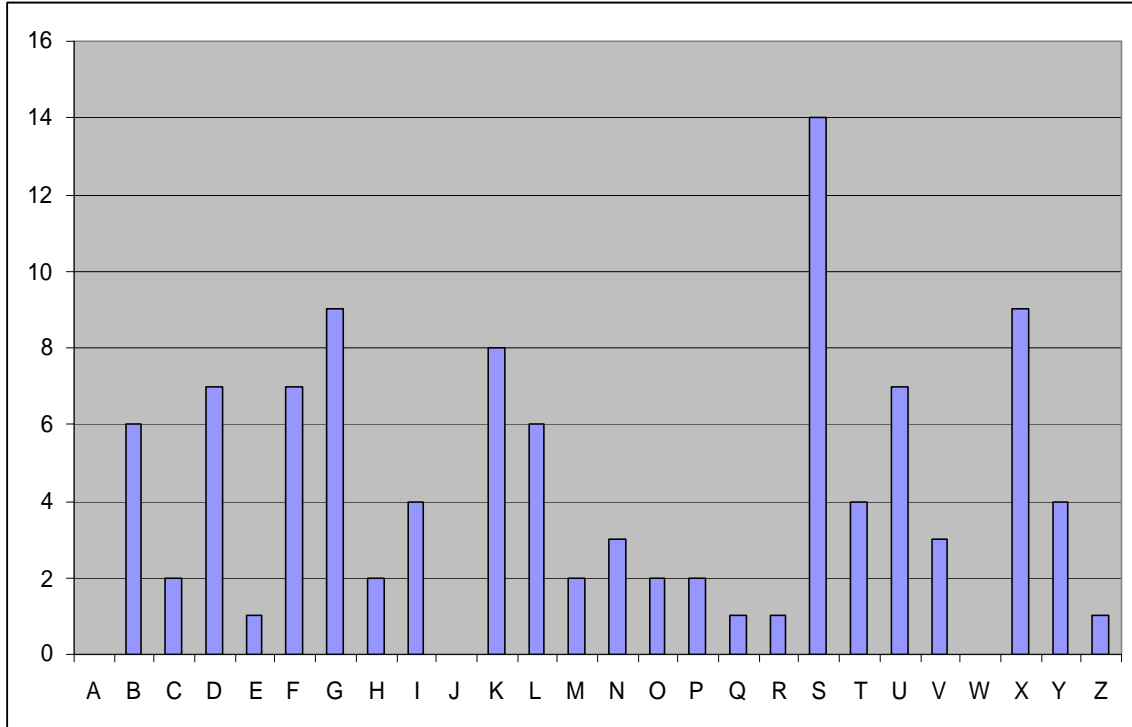

#### 9. Classic Cryptography – Monographic statistics analysis [6]

**Question A:** Below the monogram statistics for two different texts is given. One of the texts was encrypted using a Caesar -cipher and one with a substitution cipher. Decide which of the texts that were encrypted by a shift cipher. Motivate your answer (2p)

Text 1:



Text 2:



**Question B:** Calculate the index of coincidence for one of the texts based on the given statistics above (4p)

## 10. Classic Cryptography - Breaking a system [5]

The cipher text below is encrypted with a reciprocal substitution cipher. In table 1 you can see the number of occurrences of each character in the cipher text. Table 2 shows how common different letters are in the English language. The bold letter F in the cipher text below is the letter S in the plain text. Start the decryption process of this cipher text. Find at least nine more substitutions besides  $F \rightarrow S$ . You do not have to decrypt the text. (5p)

MOBUE WOLIQ OUOYN YVAPZ YFBOP POQIE CGQOE VOESP ZOSOM UZEFO  
 VPENY FYPCF GPPZO SYSPZ VOJPW EVPZG VKPGD OTGQP ESPZO OBOUP  
 YEVTQ EUOF**F** MOZET OPZGP IECZG NOPZO TEFY LYBYP IPEAY NOCFP  
 ZOTBO GFCQO ESIEC QUEWT GVIGV KPZGP IECGU UOTPP ZOZEV ECQGF  
 MOBBG FPZOQ OFTEV FYLYB YPIES PZYFG FFYAV WOVPP ZYFIO GQPZO  
 WOOPY VAMYB BPGDO TBGUO GPDOV FYVAP EVVYV OPGDO PZOLC FPZQO  
 OZCVK QOKPM OBNOF ONOVF PGPYE VFSQE WPZOU OVPQG BDOOT PZOGK  
 KQOFF GFMOB BGFpz OKGIG FOUQO PLOFP QOAGQ KF

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Occurrences	6	15	10	5	25	30	28	0	10	1	8	5	7
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Occurrences	6	61	47	18	0	8	10	11	23	6	0	22	25

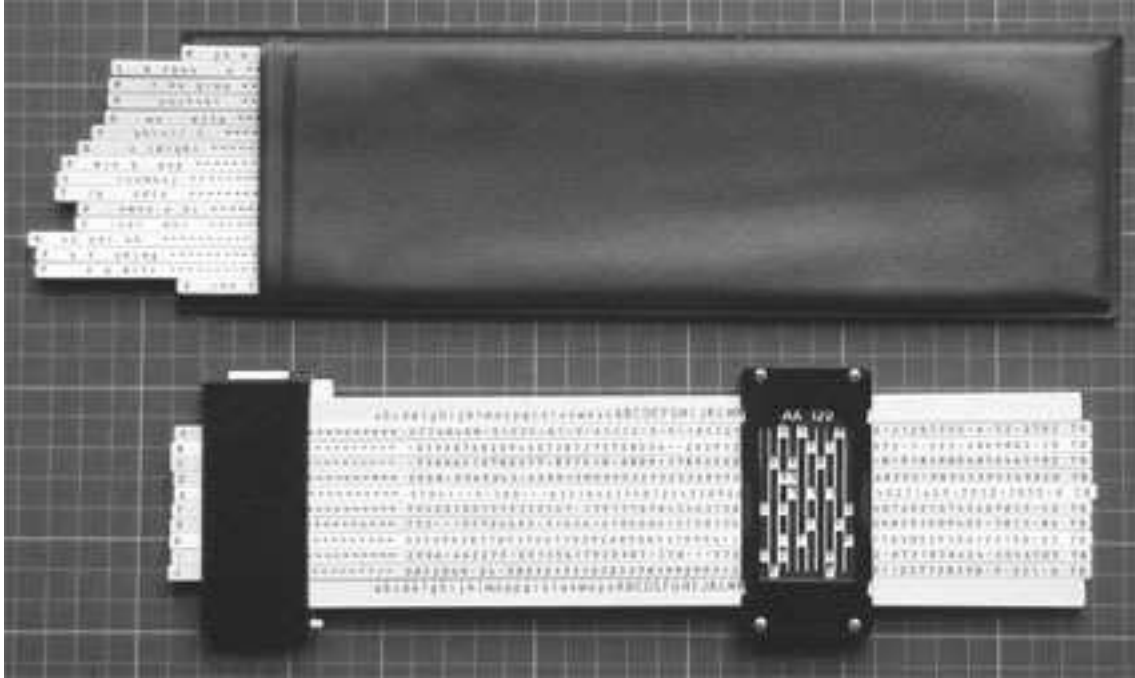
**Table 1: Frequencies of letters in cipher text**

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency	.082	.015	.028	.043	.127	.022	.020	.061	.070	.002	.008	.040	.024
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	.067	.075	.019	.001	.060	.063	.091	.028	.010	.023	.001	.020	.001

**Table 2: Frequency of letters in English**

## 11. Evaluation of a cipher system [5]

In 1950-1960 West Germany used a paper-and-pencil system to encrypt messages. It was called the Reihenschieber. The system here described can be seen as a somewhat simplified version of that cipher system. The picture below shows a slide ruler with 10 sticks fastened on it and a grille that were moved over the ruler. The grille has holes from which values were read that was used in the encryption process. The bag contains the sticks not used in this specific encryption.



Each user of the system had access to 26 sticks. The sticks were labelled from A to Z. Each stick had 4 sides. Each side consisted of 10 characters being a letter or a space, 10 holes and 70 characters being either a number from 0 to 9 or a dot. The figure below shows how the four sides of a stick could look. The example shows the stick A.

<b>A</b>	_py_x_q_r_	○ ○ ○ ○ ○ ○ ○ ○ ○ ○	24619.43.529.6565.3471.52.40
<b>A</b>	u_mvjo_zt_	○ ○ ○ ○ ○ ○ ○ ○ ○ ○	.95190.317.45602.12995.138.4
<b>A</b>	ek_lbd_c_s	○ ○ ○ ○ ○ ○ ○ ○ ○ ○	437.1512.44691.703977.69.405
<b>A</b>	_nh_gfi_aw	○ ○ ○ ○ ○ ○ ○ ○ ○ ○	2026.19.5113.4072.6198.20541

The sticks were placed on a slide ruler. How the sticks were placed was decided by 10 letters. These should be placed above each other. Assume for instance that the ten sticks used were the ones labelled X, E, G, P, V, A, W, C, T and J. Also assume that the placement are decided by the ten letters r, j, o, a, m, r, z, l, c and w. The sticks will then be positioned on the ruler in the following manner:

<b>X</b>	u_ae_l_pr		1701.5433.626.90512.3
<b>E</b>	_i_qj	○ ○ ○	849.216.55.1034.2
<b>G</b>	m_uwi__o	○	65.20473.12.9.14156
<b>P</b>	_a	○ ○ ○ ○ ○ ○ ○	9.250.3961490
<b>V</b>	oi_u_xm	○ ○	131.6150492.747318
<b>A</b>	_py_x_q_r	○	24619.43.529.6565.34
<b>W</b>	hwm_z	○ ○ ○ ○ ○	5.1693.40453.112
<b>C</b>	_i_eqrl	○ ○ ○	87.21295.306172.91
<b>T</b>	c	○ ○ ○ ○ ○ ○ ○ ○ ○ ○	.40541.331.6
<b>J</b>	u_mtnw	○ ○ ○ ○	259.10129.6542.3

On the ruler the grille is situated. The grille has 25 holes, each showing a character (either a digit or a dot). The grille is at first placed so far to the left as is possible while still characters are visible also in the leftmost holes. The characters from the holes in the grille is used in the encryption process, then the grille is moved one step and new characters appear in the holes.

90512.3	7	4	.39676.	
.1034.2	6	.	.6542.3	
9.14156	4	.	3	912.738
3961490	0	7	55.079.	
.747318	9	2	5	3.11386
6565.34	.	5	.	.40.377
453.112	.	3	827143.	
6172.91	4	3	614.45.	
1.331.6	1	.	8	.520.10
.6542.3	8	4	1	26570.1

The values seen in the holes of the grille above create the sequence:

6944870142537331458

These values are used to decide which of 20 different predetermined substitution alphabets that should be used to encrypt the text. Assume that the alphabets were labelled with a digit from 0 to 9 and with either “high” or “low”. The alphabet chosen to encrypt a letter was decided by the values in the sequence; the first value decides the digit while the second decides “low” if the value is 0 to 4 and “high” if the values is 5 to 9.

The sequence above decides the substitution alphabets. For the encryption of the first letter in the message, the first two digits in the sequence (position 1 and 2) are used to decide the alphabet labelled 6-high. For the encryption of the second letter in the message the digits in position 2 and 3 are used to decide substitution alphabet, the second one chosen is 9-low. The first ten alphabets used are then:

{6-high, 9-low, 4-low, 4-high, 8-high, 7-low, 0-low, 1-low, 4-low, 2-high}

Assume that the following is common knowledge and the same for all users of the cipher system, and therefore not part of the key of the system:

- The way each stick looks. That is the stick A always looks according to the picture above.
- The twenty substitution alphabets used.
- How the holes in the grille are situated.

**Question A:** Decide the number of keys of the encryption system. (3p)

**Question B:** What could be the reason to not only have digits on the sticks but also dots that did not contribute to the sequence used to decide substitution alphabets? (2p)

## 12. Theoretical Security [4]

Suppose we want to encrypt an English text with 112-bit 3DES. Assume that English has 70% redundancy. How many characters can a message consist of and still be considered theoretically secure? (4p)

## 13 Asymmetric encryption with RSA [4]

User A has the public key  $\{e = 17, n = 8633\}$  and the private key  $\{d = 497, n = 8633\}$ . User B has the public key  $\{e = 23, n = 8989\}$  and the private key  $\{d = 6887, n = 8989\}$ .

**Question A:** The User B signs the hash  $H$  and sends it to the user A. User A receives 2531. What is the hash value  $H$ ? (2p)

**Question B:** The User A encrypts the message  $M$  and sends it to user B. User B receives 6463. What is the message  $M$ ? (2p)

## 14. Randomness [5]

Rock, paper, scissors is a game that consists of two players. Both players choose simultaneously one of three choices: the rock, the paper or the scissors. The game can end in either player 1 winning, player 2 winning or in a draw. The game ends in a draw if both players have chosen the same alternative, i.e. if both players chose rock, both chose paper or both chose scissors.

If the two players have chosen differently the winner is:

- The player who chose rock if the other player chose scissors, since stone smashes scissors.
- The player who chose paper if the other player chose stone, since paper covers rock.
- The player who chose scissors if the other player chose paper, since scissors cut paper.

Suppose we want to make a computer program which plays the game against a human player. If we let the computer randomly choose one of the three alternatives the computer and the human player ought to win as many times, given that good randomness is used. Now suppose we want to create a computer player that should win more often than the human player. As the human player might choose alternatives in a manner that are not really random but biased the computer player will try to use this to get a larger chance of winning.

Assume that we implement the computer player strategy in the following manner. The computer keeps track of the number of times each alternative has been chosen by the human player, and then biases his own choice according to the bias of the human player. For instance assume that the human player has played with the following bias: 40% rocks, 25% paper and 35% scissors, the computer player will then choose according to the following probability distribution:

- $p(\text{rock}) = 0.35$
- $p(\text{paper}) = 0.4$
- $p(\text{scissors}) = 0.25$

**Question A:** Assume that the human player knows the implementation of the computer player, i.e. the rules of the strategy. Describe the weakness in the algorithm by describing how the human player can make choices to win more often than the computer player. (3p)

**Question B:** Discuss whether it is possible to improve the computer player. If it is, how this is done. (2p).