



Cryptography

Exercises

January 31, 2023

Problems

Read each of the following problems and solve them. Please include all your calculations

1. Suppose that we are using the following association between each letter in the german alphabet and an the set $\{0, 1, \dots, 29\}$:

A \leftrightarrow 0	B \leftrightarrow 1	C \leftrightarrow 2	D \leftrightarrow 3	E \leftrightarrow 4	F \leftrightarrow 5
G \leftrightarrow 6	H \leftrightarrow 7	I \leftrightarrow 8	J \leftrightarrow 9	K \leftrightarrow 10	L \leftrightarrow 11
M \leftrightarrow 12	N \leftrightarrow 13	O \leftrightarrow 14	P \leftrightarrow 15	Q \leftrightarrow 16	R \leftrightarrow 17
S \leftrightarrow 18	T \leftrightarrow 19	U \leftrightarrow 20	V \leftrightarrow 21	W \leftrightarrow 22	X \leftrightarrow 23
Y \leftrightarrow 24	Z \leftrightarrow 25	Ä \leftrightarrow 26	Ö \leftrightarrow 27	Ü \leftrightarrow 28	ß \leftrightarrow 29

We will encipher each message with the following equation:

$$e_K(m_i) = (am_i + b) \bmod n$$

where $a, b \in \{0, 1, \dots, 29\}$ and m_i is a character of the message. Answer the following questions :

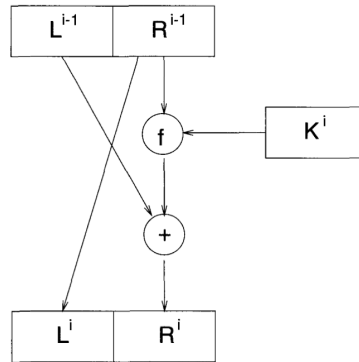
- a) Choose a valid value for a and b and then write down the equation to decipher. Calculate the value of $a^{-1} \bmod n$ with the extended euclidean algorithm. Include the details of your calculation.
 - b) List all the elements valid for a ? Justify your answer.
 - c) Determine the number of possible keys, consider that the key is the pair (a, b) .
2. Consider the following pseudocode (Algorithm1) where M is the plaintext, K is a secret key, IV is a random value, C is the ciphertext. Answer the following questions
 - a) What is the name of the procedure described in the pseudocode?
 - b) Write down the pseudocode to reverse the previous procedure. It must receive as input C, K, IV and must recover M .
 - c) Explain why the IV must be random, and must change every time we encipher a message.

```

Algorithm1( $M, K, IV$ )
1. Partition  $M$  into  $M_1, M_2, \dots, M_n$ 
2.  $C_1 \leftarrow E_K(M_1 \oplus IV)$ ;
3. for  $i \leftarrow 2$  to  $n$ 
4.    $C_i \leftarrow E_K(M_i \oplus C_{i-1})$ ;
5. end for
6. return  $C_1, C_2, \dots, C_n$ 

```

3. Look at the following figure



- a) What are its components, i.e, explain what is $L^{i-1}, R^{i-1}, f, K^i, L^i, R^i$?
 - b) Write down the mathematical expression for L^i and R^i .
 - c) Give the name of a block cipher that uses this structure in its design.
4. In certain organization are using RSA to encipher sensitive data. Imagine that you are an adversary who has captured the following information: $n = 3127$, the RSA public key $e = 2413$, and the ciphertext $c = 3122$.
 - a) What would be the private key d ? Please include in detail all your calculations
 - b) Using the private key that you previously discovered, find the plaintext m corresponding to c
5. The security of some cryptographic systems is based on the hardness of the discrete logarithm problem
 - a) Explain what is the discrete logarithm problem in \mathbb{Z}_p^* , i.e, in the multiplicative group of integers mod n .
 - b) Consider the Diffie-Hellman protocol. Imagine that you are an adversary eavesdropping the channel, and you have the following values: the prime number $p = 31$, the generator $g = 3$, and see that Alice sent to Bob the value $y_A = 19$ and the value that Bob sent to Alice $y_B = 26$. Given this information, find the key K .