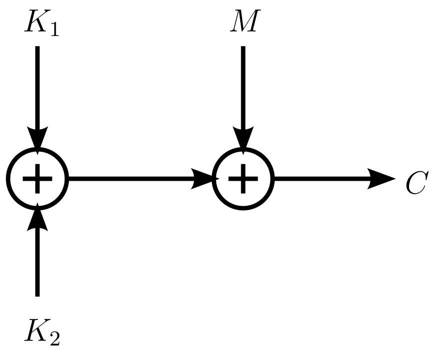
Review Exercise
Cryptography I

Prof. Dr. Rudolf Mathar, Michael Reyer, Georg Böcherer, Steven Corroy, Henning Maier

01.08.2011, WSH 24 A 407, 14:00h

Problem 1.



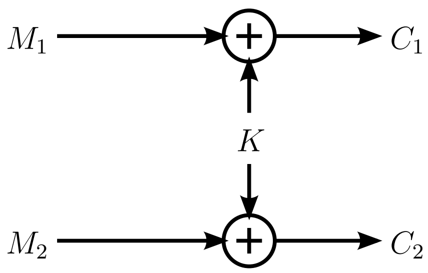
In the encryption system above, the message M and the two keys K_1 and K_2 are binary valued in $\{0, 1\}$ and addition is taken modulo 2. The message M and the key K_1 are uniformly distributed. The key K_2 has the distribution $P(K_2 = 0) = p$, $P(K_2 = 1) = 1-p$, $0 < p < \frac{1}{2}$. M, K_1, and K_2 are stochastically independent. Use dual logarithm in your calculations.

(a) Derive the distribution of $K_1 \oplus K_2$ and derive the distribution of C.

(b) For which values of p does the system have perfect secrecy?

(c) Show that the message equivocation $H(M|C)$ is greater than the key equivocation $H(K_2|C)$.

Consider now the following system.



The message is $\boldsymbol{M} = (M_1, M_2)$ and the ciphertext is $\boldsymbol{C} = (C_1, C_2)$. M_1 and M_2 are binary and uniformly distributed. The key K is also binary and uniformly distributed. M_1, M_2, and K are stochastically independent. The addition is modulo 2.

(d) Specify the encryption function e and the decryption function d of the displayed system. Does this system satisfy the formal definition of a cryptosystem?

(e) Calculate the equivocations $H(M_1|C_1)$ and $H(M_2|C_2)$.

(f) Does the system have perfect secrecy?

Problem 2.

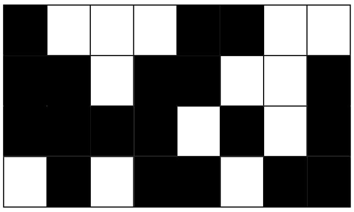


Figure 1: Encrypted picture C

IP							
8	7	6	5	1	2	3	4
13	14	15	16	9	10	11	12
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

Figure 2: Initial permutation IP

The 4×8 pixels of the encrypted picture in Figure 1 are numbered as $C = (c_1, \ldots, c_{32})$ from top-left to bottom-right, row by row. A black pixel has the binary value one and a white pixel the value zero. In the following, all numbers are given as hexadecimal values.

The encryption procedure of the used block cipher has the following structure:

(1) Four 8-bit subkeys $K_1, \ldots, K_4$ are generated from a 16-bit key $K = (k_1, \ldots, k_{16})$. For subkey $K_1 = (k_{1,1}, \ldots, k_{1,8})$, first, expansion E is applied to $k_1, \ldots, k_4$. Then, S-box S_1 is applied on the first four bits of the output, providing bits $k_{1,1}$, $k_{1,2}$ and on the last four bits providing $k_{1,3}$, $k_{1,4}$, respectively. Analogously, S-box S_2 is used for bits $k_{1,5}$, $k_{1,6}$ and $k_{1,7}$, $k_{1,8}$. The first two bits specify the row, the last two bits the column of the S-box. The remaining subkeys are computed from $k_5, \ldots, k_{16}$.

$$E : (4\ 1\ 2\ 3\ 2\ 3\ 4\ 1),\ S_1 = \begin{pmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix},\ S_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 2 & 0 & 3 \end{pmatrix}$$

(2) The initial permutation (IP) given in Figure 2 is applied to the 32 input bits M. The output is denoted by $\widehat{M}$.

(3) Each row $i = 1, \ldots, 4$ of 8 bits is considered as a submessage $\widehat{M_i}$ of $\widehat{M}$. The $\widehat{M_i}$ are encrypted according to the *counter mode*. The encryption function of a 8-bit value X is given as $E_{K_i}(X) = \mathrm{ROTL}(X \oplus K_i, 4, 8)$. The operation $\mathrm{ROTL}(W, k, n)$ is defined as cyclic left shift of k-bits of an n-bit input W. The output is $\widehat{C}$.

(4) The inverse permutation IP^{-1} is applied to the 32 output bits $\widehat{C}$ of step (3). The output generated here is the final ciphertext C.

Solve the following problems:

(a) Generate the first subkey K_1 from $K = 0xB47F$ as described in step (1).

(b) Compute the inverse permutation IP^{-1} to the given IP.

(c) Specify the corresponding decryption procedure of this block cipher. Omit the key generation, i.e., subkeys $K_1 \ldots, K_4$ may be utilized directly.

(d) Decipher the encrypted image of Figure 1 using the following new subkeys $K_1 = 0x39$, $K_2 = 0x64$, $K_3 = 0x77$ and $K_4 = 0x1C$. The initial counter value is set to value $Z_1 = 0x4C$. Furthermore, use Figure 3 for your solution.

(e) What other modes of operation do you know?

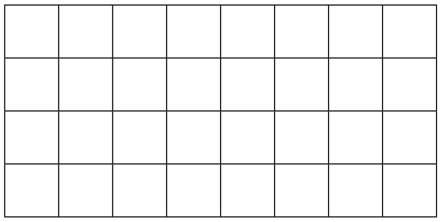


Figure 3: Decrypted picture

Problem 3.

Alice and Bob use RSA to exchange information. Bob generates two numbers $p = 11$ and $q = 349$ and calculates $n = pq$.

(a) The numbers p and q must be prime. Bob wants to check their primality using the Miller-Rabin primality test. Show that 3 is not a strong witness for the compositeness of q. Can you conclude that q is prime?

(b) Bob chooses the private exponent $d = 37$. Calculate the public exponent e of Bob.

(c) Alice wants to send the message $m = 44$ to Bob. Determine the ciphertext c transmitted by Alice.

Bob transmits several messages $(m_1,\ m_2,\ \ldots)$ to Alice using the public key $n = 119$. For each message m_i, Bob uses the exponents (d_i, e_i). Eve wants to decrypt the communication between Alice and Bob. Eve has an oracle which returns the correct decryption exponent d given e and n.

(d) Explain how Eve can use the oracle to determine p and q.

(e) Compute p and q given $d_1 = 5$ corresponding to $e_1 = 77$ and $d_2 = 13$ corresponding to $e_2 = 37$.