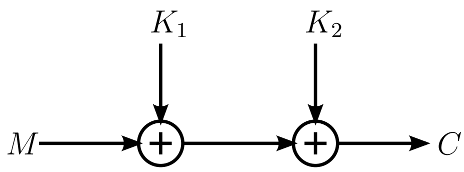
Review Exercise for Cryptography and Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Georg Böcherer, Henning Maier

01.03.2011, WSH 24 A 407, 14:00h

Problem 1.



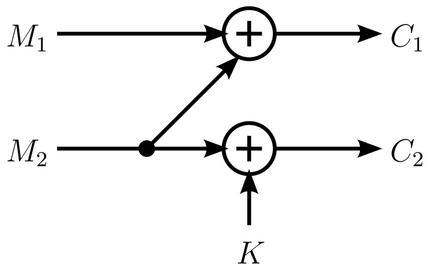
In the encryption system above, the message M and the two keys K_1 and K_2 are binary and addition is taken modulo 2. The message M is uniformly distributed. The key K_1 has the distribution $P(K_1 = 0) = p$, $P(K_1 = 1) = 1 - p$, $0 < p < \frac{1}{2}$ and the key K_2 has the distribution $P(K_2 = 0)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

(a) Assume $q = 1$. Show that the message equivocation $H(M|C)$ is equal to the key evocation $H(K_1|C)$.

(b) Derive the distribution of $K_1 \oplus K_2$ in terms of p and q.

(c) Show that the system has perfect security if and only if $q = \frac{1}{2}$.

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 jointly stochastically independent. The addition is modulo 2.

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

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

(f) Calculate the equivocation $H(\boldsymbol{M}|\boldsymbol{C})$. Has the system perfect security?

Problem 2.

Alice and Bob use the Diffie-Hellman key exchange protocol with the prime number $p = 107$ and the primitive element $a = 2$. Alice chooses the random number $x_A = 66$, and Bob chooses $x_B = 33$.

(a) Compute the common shared key. Give the intermediate calculations.

(b) Show that $b = 103$ is also a primitive element.

(c) What is the common shared key if Alice und Bob use the primitive element 103?

Problem 3.

Bob uses RSA with the public key $(e, n) = (7,\ 11{\cdot}13)$.

(a) What is Bob's private key?

(b) Alice encrypts $m_1 = 110$ with Bob's public key (e, n). What is the encrypted message c_1?

(c) Alice encrypts the message m_2 for Bob with his public key (e, n). Bob receives the encrypted message $c_2 = 10$. What was the original message m_2 from Alice?

Alice uses RSA and has the public key $(e', n') = (9, 253)$ and the private key $d' = 49$. Eve knows the public key (e', n') and she also gets to know the private key d'.

(d) With Eve's knowledge, calculate a multiple x of $\varphi(n')$ in $\mathbb{Z}$, i.e., some $x \in \mathbb{Z}$ such that $x = k \cdot \varphi(n')$ for some $k \in \mathbb{N}$.

(e) Calculate the prime factorization in $\mathbb{Z}$ of x from (d).

(f) Use the result from (e) to find the factors k and $\varphi(n')$ of x and the prime factors p and q of n'.

Problem 4.

Alice wants to sign a message $m = 77$ using the ElGamal signature scheme without using a hash function. She uses the public prime $p = 97$ and the parameter $a = 5$.

(a) Which condition must be fulfilled by a to be used in the ElGamal signature scheme? Show that $a = 5$ fulfills this condition

(Hint: $5^{48} \pmod{97} \equiv 96$ and $5^{32} \pmod{97} \equiv 35$).

(b) Alice chooses the private key $x_A = 8$ and picks the random secret $k = 7$. Give the signature (r, s) of the message $m = 77$.

The ElGamal signature scheme is weak against the following attack. Given two integers u and v with

$$\begin{aligned} &\gcd(v, p-1) = 1, && r = a^u y_A^v \pmod{p}, \\ &s = -rv^{-1} \pmod{p-1}, && m = -ruv^{-1} \pmod{p-1}. \end{aligned}$$

(c) Show that (r, s) is a valid ElGamal signature on m.

(d) With this method Eve can produce signatures on random documents. Show that Eve cannot use this method anymore if a hash function h is used by Alice and the signature must be valid for $h(m)$ instead of m.

There exist many variations of the ElGamal signature scheme which do no compute s as $s = k^{-1}(m - x_A r) \bmod (p-1)$.

(e) Consider the signing equation $s = x_A^{-1}(m - kr) \bmod (p-1)$. Show that the verification $a^m \equiv y_A^s r^r \pmod{p}$ is a valid verification procedure.

(f) Consider the signing equation $s = x_A m + kr \bmod (p-1)$. Show that the verification $a^s \equiv y_A^m r^r \pmod{p}$ is a valid verification procedure.

(g) Consider the signing equation $s = x_A r + km \bmod (p-1)$. Propose a valid verification procedure.

Problem 5.

Consider the Lamport authentication protocol.

(a) Describe the Lamport authentication protocol. On which problem is its security based?

(b) Assume Oscar controls the link between Alice and Bob. How can Oscar impersonate himself to Bob as Alice?

As an improvement, authentication shall be performed by a Challenge-Response (CR) protocol.

(c) Describe a mutual CR-authentication protocol based on signatures.

For the protocol, a signature must be created. Use a DSA signature with artifically small values for signing the message with the hash value $h(m) = 12$. You know the public parameters $p = 137, q = 17, a = 3, y = 136$. Proceed as follows:

(d) Find the private key x from the public key y.

(e) Sign the hash value using the session key $k = 3$.

Problem 6.

Consider the elliptic curve

$$E : y^2 = x^3 + 2.$$

The curve is defined over $\mathbb{F}_5$.

(a) Calculate all points of the curve. How many points are in $E(\mathbb{F}_5)$?

(b) Identify the inverses $-P$ for all points $P \in E(\mathbb{F}_5)$.

Now the elliptic curve ElGamal signature scheme is performed on $E(\mathbb{F}_5)$ with the generator $P = (4, 1)$. Alice's public key is $(3, 3)$. Assume that messages m are encoded by some point on the curve, whose y-coordinate is m.

(c) Sign the message $m = 1$ using $k = 2$.

(d) Is $P = (2, 0)$ a generator for $E(\mathbb{F}_5)$?