Exam - Cryptology 1 - 01410

May 19, 2021

Exam - Cryptology 1 - 01410, May 19, 2021

Start 09.00 Denmark time. End 13.00.

This exam counts for 70% of the final grade, the homeworks count for the remaining 30%. The first two exercises below count for 5% each, the remaining 6 exercises for 10% each.

Write down your results and save them in a PDF document, and upload it to the DTU system, before the deadline.

Exercise 1 State whether the following statements are true or false (T/F).

1. Cryptographic hash functions are mainly used for public-key encryption.
2. A MAC algorithm needs to be invertible.
3. In differential cryptanalysis one does an exhaustive search for the key.
4. The Diffie-Hellman protocol was the first public-key encryption system in the world.
5. A secret sharing scheme is used only for public-key authentication.
6. AES is a public-key cryptosystem.
7. An output from the Miller-Rabin algorithm is a provable prime.
8. Non-repudiation is where the opponent cannot determine the key.
9. HMAC is used for symmetric authentication.
10. RSA cannot be broken by any adversary.

Exercise 2
Consider the square-and-multiply method for computing exponentiations modulo m, where m is a large, positive integer. Show how many modular squarings and how many modular multiplications are required to compute

1. $x^{219} \bmod m$.
2. $x^{319} \bmod m$.

Exercise 3 Consider RSA encryption with a modulus $n = p \cdot q$, where p and q are two odd, distinct primes, e is the public exponent and d the private exponent. With RSA encryption, it is common practice to choose e as a small number (e.g., $3, 11, 17$).

1. Explain why it could be an advantage to choose one of these exponents?

2. If you wanted to make decryption faster, instead of encryption, you could set d to one of above three values and compute the corresponding value of e. Argue why this is not a good idea.

3. Recall that $\mathbb{Z}_n^*$ are the numbers m, for which $\gcd(m, n) = 1$. Show why RSA works for messages $m \in \mathbb{Z}_n^*$, that is, show that $(m^e)^d \equiv m \bmod n$.

4. Let $n = 9307$ be an RSA modulus and let $e = 3$. Calculate the decryption of the ciphertext $c = 4151$.

Exercise 4

1. Calculate
$$4^{12}6^{24} \bmod 77$$
in a clever way using Fermat's theorem and the Chinese Remainder Theorem. Show the individual steps in the calculations.

2. Calculate
$$4^{12}6^{24} \bmod 64.$$
Show the individual steps in the calculations.

Exercise 5

Consider block ciphers and modes of operation. The block cipher encrypts an n-bit block m_i into an n-bit ciphertext block c_i using a key k, that is,

$$e_k(m_i) = c_i.$$

Decryption is defined

$$d_k(c_i) = m_i.$$

In a mode of operation the ciphertext blocks are encrypted as follows

$$c_i = e_k(m_i \oplus c_{i-1}) \oplus m_{i-1}$$

for $i = 1, 2$, etc., and where m_0 and c_0 are constants.

1. Show how the decryption operation should be.

2. Discuss how an (transmission) error in a single block of a received ciphertext will affect the decryption operation.

Exercise 6
Consider a $(3, 21)$-threshold secret sharing system, where $p = 53$ (a prime). Three shareholders have the following pairs (x_i, y_i): (1,7), (3,9), and (2,4).

1. Find the secret key k

Exercise 7 Let p be a large prime, and let α be a primitive element in $\mathbb{Z}_p$ such that DLP(p) is considered difficult.
Define the hash function $H : \mathbb{Z} \to \mathbb{Z}_p$ as follows

$$H(x) = \alpha^x \bmod p.$$

Evaluate this hash function with respect to

1. collision attacks,
2. second preimage attacks,
3. preimage attacks.

Exercise 8
Consider the following variant of El-Gamal signature system, where H is a public hash function.

Public key: An odd prime p, primitive element $\alpha \in \mathbb{Z}_p^*$, $\beta = \alpha^a \bmod p$.

Private key: $a \in \mathbb{Z}_{p-1}$.

Signature: Let m be a message and let $x = H(m) \in \mathbb{Z}_{p-1}$. The signature of m is (γ, δ), where k is randomly chosen from $\mathbb{Z}_{p-1}$ and where

$$\begin{aligned} \gamma &= \alpha^k \bmod p \\ \delta &= a \cdot \gamma + k \cdot x \bmod (p-1) \end{aligned}$$

Verification: Let m be a message and let $x = H(m)$.
$(\gamma, \delta) \in \mathbb{Z}_p \times \mathbb{Z}_{p-1}$ is accepted as the signature on m if

$$\alpha^\delta = \beta^{???} \gamma^{???} \bmod p.$$

1. Complete the verification process. How is a signature verified as valid?
2. Find one advantage of this variant of the El-Gamal signature system compared to the original.

NB. The security of this variant of the El-Gamal signature system has been shown to be equal to the security of the original system.