University of Science and Technology of Hanoi *** **Final Examination** Subject: Introduction to Cryptography **Exam code: 10** Number of pages: 02	Intake: BI10+BI11 Academic year: 2021-2022 Date: 26/02/2022 Time: 75 minutes **Important instructions:** - One-sided A4 page handwriting note are allowed - Laptop is allowed

Exercise 1 (6/20)

Implement the A5/1 algorithm. Suppose that, after a particular step, the values in registers are

$X = (x_0, x_1, ..., x_{18}) = (0110011001100110011)$

$Y = (y_0, y_1, ..., y_{21}) = (1101110111011101110111)$

$Z = (z_0, z_1, ..., z_{22}) = (11010001101000110100011)$

The first keystream bit is computed with the initial values of the registers. List the next 3 keystream bits (including the first keystream bit, left first. Give the contents of X, Y, and Z after these 3 bits have been generated.

Exercise 2 (4/20)

Following hash function is built from block cipher with the encryption $e()$. Draw its block diagram:

$$H_i = e(x_i \oplus H_{i-1}, x_i) \oplus H_{i-1}$$

Exercise 3 (4/20)

In RSA cryptosystem:

1. Describe key generation, encryption and decryption.

2. Let the two primes $p = 211$ and $q = 97$ be given as set-up parameters for RSA. Which of the parameters $e_1 = 91, e_2 = 89$ is a valid RSA exponent? Justify your choice.

3. Compute the corresponding key-pair from above parameters. Using this keypair to encrypt and decrypt plaintext: $M = 5022$

p, q are prime numbers, modulus $N = p*q$, e denotes encryption exponent, M denotes the plaintext.

Exercise 4 (6/20)

Consider the Elgamal signature scheme:

You are given Bob's private key $K_{pr} = (d) = (127)$ and the corresponding public key $K_{pub} = (p, \alpha, \beta) = (509, 2, \beta)$.

1. Calculate the Elgamal signature (r,s) for a message from Bob to Alice with the following messages x and ephemeral keys k_E:

$$x = 8022, k_E = 215$$

2. Two messages x_1, x_2 are received with their corresponding signatures (r_i, s_i) from Bob. Verify whether the messages $(x_1, r_1, s_1) = (22, 249, 413)$ and $(x_2, r_2, s_2) = (82, 249, 342)$ both originate from Bob?

3. A given Certification Authority (CA) uses Elgamal signature scheme to generate Certifications for Alice and Bob. The two IDs for them are correspondingly ID(A)=1 and ID(B)=2. The CA uses the ephemeral keys $k_E = 213$ and 215 for A's, and B's signatures, respectively. The numbers that are chosen at each user to generate their public keys (using Diffie-Helman Key Exchange scheme) are:

$$b_A = 2022,\ b_B = 2602$$

To obtain the certificates, the CA computes $x_i = 4 * b_i + ID(i)$ and uses this value as input for the signature algorithm. Compute and verify two certificates CertA and CertB.

The End - Good Luck!