

**ECE 746 Midterm Exam 1**  
**November 1, 2006**

**Multiple-choice test**

**1. (1 pt) Match listed below cryptosystems into pairs of cryptosystems with the equivalent security:**

- A. Rijndael with the key size 256 bits
- B. ECC-DSA with the key size 224 bits
- C. ECC with the key size 512 bits
- D. RSA with the key size 2048 bits
- E. Skipjack
- F. DSA with the key size 1024 bits

**2. (1 pt) Precomputations, i.e., computations that can be performed before input data (e.g., message) becomes available, can be used to speed up the following cryptographic transformations (please list ALL correct solutions):**

- A. RSA signature verification
- B. encryption in the El-Gamal encryption scheme
- C. DSA signature generation
- D. decryption using the RC4 cipher
- E. encryption using stream cipher based on the shrinking generator
- F. decryption in the Menezes-Vanstone Elliptic Curve Cryptosystem

**3. (1 pt) Using look-up tables included in the reference implementation of Rijndael perform multiplication '0F'·'FF' in  $GF(2^8)$ . The result of this operation is (all numbers in the hexadecimal notation):**

- A. '0A'
- B. '10'
- C. '2E'
- D. '46'
- E. '72'
- F. none of the above

**4. (1 pt) Which of the following elements are the generators of the group,  $\{x^i \bmod x^4+x^3+1, i=1..15\}$  with the multiplication modulo  $x^4+x^3+1$  (please list ALL correct solutions):**

- A.  $x^2$
- B.  $x^3$
- C.  $x^4 \bmod x^4+x^3+1 = x^3+1$
- D.  $x^5 \bmod x^4+x^3+1 = x^3+x+1$
- E.  $x^6 \bmod x^4+x^3+1 = x^3+x^2+x+1$

**5. (1 pt) Random bits are required in the following transformations (please list ALL correct answers):**

- A. generation of system parameters in EC-DSA
- B. verification of a signature in DSA
- C. generation of a signature in RSA
- D. encryption in the Menezes-Vanstone Elliptic Curve Cryptosystem
- E. generation of keys in RSA

**6. (1 pt) The total size of tables T used in the optimized software implementation of Rijndael capable of performing both encryption and decryption, in the counter mode, in the shortest amount of time is:**

- a. 1 kB
- b. 2 kB
- c. 4 kB
- d. 8 kB
- e. other (give value)

**7. (1 pt) The ratio of the time necessary to encrypt data vs. time necessary to decrypt data in the Elliptic Curve El-Gamal Cryptosystem is equal approximately to (assume that no precomputations are used during either of the two transformations):**

- A. 0.25
- B. 0.5
- C. 1
- D. 2
- E. 4
- F. other (give value)

**8. (1 pt) The linear complexity of the sequence 110110 is equal to**

- A. 0
- B. 1
- C. 2
- D. 3
- E. 4
- F. 5
- G. 6

### Short problems

1. (3 pts) Compute  $T_3[2]$ , i.e., the contents of the look-up table  $T_3$ , used in the optimized implementation of the Rijndael encryption, at position 2. Show all intermediate steps of your computations. Write a formula for the column number  $j=3$ , in the output of the 5<sup>th</sup> round of AES, with the key size equal to 128 bits, using look-up tables  $T_0$ ,  $T_1$ ,  $T_2$ , and  $T_3$ .
2. (3 pts) Find the shortest Linear Feedback Shift Register and its initialization that produce the keystream “11010111”.
3. (3 pts) Create a table of logarithms and antilogarithms with the logarithm base  $x+1$  that can be used to speed up computations in the Galois field  $GF(2^3) = \{Z_2[x]/x^3+x+1, \text{polynomial addition modulo } x^3+x+1, \text{polynomial multiplication modulo } x^3+x+1\}$ . Show how to use these tables to compute values of the following expressions in  $GF(2^3)$ . Verify your solutions to the points a. and b. by performing the same computations using another method known to you.

- a. '7' · '6'
- b. '3'<sup>-1</sup>
- c. '5' · '4'<sup>-1</sup>

4. (3 points) Using Elliptic Curve El-Gamal Cryptosystem with

system parameters:

$E: y^2 = x^3 + x + 6$  over  $GF(11)$ ,  $\#E(GF(11))=13$ , and  $P=(2, 7)$

private key of the sender:  $x_S = 5$

public key of the sender:  $Y_S = (3, 6)$

private key of the receiver:  $x_R = 9$

public key of the receiver:  $Y_R = (10, 9)$

encrypt message  $M=5$ .

Choose random value of  $k$  in such a way to reduce the amount of necessary computations, but at the same time make  $k$  different than 1 and 13.

5. (3 pts) Encrypt the word “PM” (ASCII codes 50 4D in the hexadecimal notation) using the shrinking generator with the component LFSRs  $R_1 = \langle 3, 1+D+D^3 \rangle$ ,  $R_2 = \langle 5, 1+D^3+D^4 \rangle$ , and the initial states of  $R_1$  and  $R_2$  equal to  $[1,1,0]$ ,  $[1,0,0,1,0]$ , respectively.