CSCI 462 Introduction to Cryptography

Exam: Midterm Examination
Duration: 75 minutes
Instructor: Monika Polak

03/06/2019

Full Name (printed): KEY

Instructions:

- The exam contains 9 pages. The last page is a scrap paper. Please make sure you have all pages.
- The exam contains a total of 29 points.
- The midterm is closed book and notes but you may use one page with your own notes (letter-sized paper).
- If you require clarification of a question, please raise your hand.

True or False (5 points)

For each of the following statements, circle TRUE if the statement is true. Circle FALSE if the statement is false.

1. TRUE / FALSE DES is an example of Feistel Network.
2. TRUE / FALSE $11_{Hex} \oplus FF_{Hex} = EE_{Hex}$.
3. TRUE / FALSE AES is a byte-oriented cipher.
4. TRUE / FALSE A stream cipher can be built from a block cipher.
5. TRUE / FALSE Encryption using Cipher Block Chaining mode (CBC) cannot be parallelized but decryption can be.
6. TRUE / FALSE Trivium is a secure stream cipher.
7. TRUE / FALSE Meet in the middle attack against 3DES requires 2^{113} encryptions/decryptions.
8. TRUE / FALSE Key Whitening can be used to make all weak ciphers secure.
9. TRUE / FALSE S-boxes are the only nonlinear elements of AES.
10. TRUE / FALSE A stream cipher algorithm defines how to encrypt/decrypt arbitrary-length messages.

Multiple Choice and Short Answer (11 points)

Indicate the correct response for each question.

1. (1 point) Encrypt message CAT using Caesar cipher with key $K = 10$.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Answer: MKD

2. (1 point) The sentence: "Assures that private or confidential information is not made available or disclosed to unauthorized individuals", describes:

(a) Data confidentiality
(b) Authentication
(c) Integrity
(d) Non-Repudiation

3. (1 point) Compute

$$\frac{2}{5} \; mod \; 7$$

Answer: $2 \cdot 3 \bmod 7 = 6$

4. (1 point) What is the output of the following DES S-box for the input 101011.

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Answer: 09

5. (1 point) There are elements in $\mathbb{Z}_9$ without a multiplicative inverse. Which elements are these?

Answer: 0, 3, 6

6. (1 point) Compute

$$6^{100} \cdot 12 \; mod \; 5$$

Answer: $6^{100} \bmod 5 \cdot 12 \bmod 5 = 1 \cdot 2 = 2$

7. (1 point) Let $n = 17$. Use Blum-Blum-Shub generator to compute the first 3 bits of the generated output with seed $x_0 = 5$.

Answer: 010

8. (1 point)

Given a block cipher with a key length of 80 bits and block size of 50 bits, as well as 2 plaintext-ciphertext pairs $(x_1, y_1), (x_2, y_2)$, the expected number of false keys that encrypt all plaintexts to the corresponding ciphertexts is:

(a) 2^{30}
(b) $1/2^{30}$
(c) 2^{120}
(d) $2^{80}/2^{50}$

9. (1 point) Consider permutation P:

8	1	4
6	5	2
7	9	3

Consider the following bit sequence as the input data 111 100 011. Write down the permuted output.

Answer: 111 001 011

10. (2 points) Assume a password consisting of 5 letters, where each letter is encoded by the ASCII scheme (7 bits per character, i.e., 128 possible characters).

a) What is the size of the key space that can be constructed by such passwords?

128^5

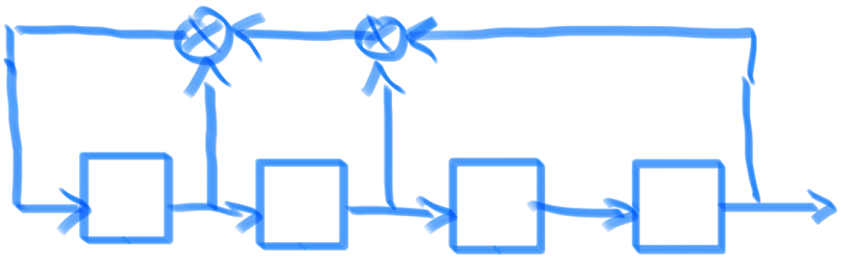
b) What is the corresponding key length in bits?

$\log_2 128^5 = 5 \log_2 128 = 35$

Open problems (13 points)

1. **(6 points = 4 + 1 +1 points)** Draw a diagram representing the linear feedback shift register (LFSR) described by the following polynomial:

$$P(x) = x^4 + x^3 + x^2 + 1.$$



a) What is the maximum sequence length generated by an LFSR of degree 4?

$2^4 - 1 = 15$

b) The LFSR is initialized with the value $(s_3, s_2, s_1, s_0) = (1, 0, 1, 1)$. What are the first three keystream bits that are generated?

				output
1	0	1	1	1
0	1	0	1	1
0	0	1	0	0

1

2. **(4 points)** Computations in $GF(2^8)$, where the irreducible polynomial is the one used by AES, $P(x) = x^8 + x^4 + x^3 + x + 1$. Let

$$A(x) = x^3 + 1, \quad B(x) = x^3 + x^2 + 1.$$

Compute:

a) $A(x) + B(x)$.

$x^3 + 1 + x^3 + x^2 + 1 = x^2$

b) $A(x) \cdot B(x)$.

$$x^3 + x^2 + 1$$
$$x^3 + 1$$
$$x^3 + x^2 + 1$$
$$+ \quad x^6 + x^5 + x^3$$
$$x^6 + x^5 + x^2 + 1$$

Show the details of your work. Your answer must be in the form of a polynomial.

3. **(3 points)** List three differences between DES and AES.

For example:

i) DES is an example of Feistel network, AES not

ii) DES key length : 64 bits
AES key length : 128, 192, 256

iii) DES is not secure
AES is secure

SCRAP PAPER