UNIVERSITY OF MASSACHUSETTS
Dept. of Electrical & Computer Engineering

Introduction to Cryptography
ECE 597XX/697XX

Sample Test Questions

Israel Koren

1. Substitution ciphers may be subject to frequency attacks. To reduce the effectiveness of such attacks groups of k (k>1) letters can be substituted individually, i.e., the plaintext is partitioned into groups of k letters each and every group is substituted separately (Hill's cipher).
(a) What would be the key size for k=2? Write an expression for the key size as a function of k (k>1) and compare it to the key size for k=1.

(b) The key size can be reduced by using a common transformation for all groups of k letters. For example, for k=2 the matrix M below can be used to substitute the pair x_1x_2 by y_1y_2.

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

The calculation is done mod 26, e.g., $y_1 = a \cdot x_1 + b \cdot x_2 \bmod 26$

Encrypt the plaintext SNOW using the matrix $M = \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix}$

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

(c) Show that the matrix M*, with h satisfying gcd(h,ad-bc)=1, can be used to decrypt the ciphertext. Verify it by decrypting the ciphertext you obtained in (b).

$$M^* = \begin{pmatrix} hd & -hb \\ -hc & ha \end{pmatrix}$$

(d) You happen to know that CD is encrypted as RR and JK as OV. Decrypt the ciphertext WGTK (*known-plaintext attack*).

(e) If you can mount a *chosen-plaintext attack*, which plaintexts would you choose?

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

2. Consider an affine cipher for the German alphabet that consists of the following letters:

(a) How large is the key space?

A ↔ 0	B ↔ 1	C ↔ 2	D ↔ 3	E ↔ 4	F ↔ 5
G ↔ 6	H ↔ 7	I ↔ 8	J ↔ 9	K ↔ 10	L ↔ 11
M ↔ 12	N ↔ 13	O ↔ 14	P ↔ 15	Q ↔ 16	R ↔ 17
S ↔ 18	T ↔ 19	U ↔ 20	V ↔ 21	W ↔ 22	X ↔ 23
Y ↔ 24	Z ↔ 25	Ä ↔ 26	Ö ↔ 27	Ü ↔ 28	ß ↔ 29

(b) The following ciphertext was encrypted using the key a=17 and b=1, what is the plaintext? LZBHH

3. Consider the long term security of AES with a key length of 128 bits.
(a) Assume that we have a special-purpose ASIC that searches 5x10^8 keys per second. One ASIC costs $50 and the circuit integration overhead is 100%. How many ASICs can be used with a $1M budget? How long will an average key search take?

(b) Future prediction based on Moore's law (computing performance doubles every 18 months at a constant price): How many years do we have to wait until breaking an AES will take 24 hours (with the same budget of $1M)?

4. (a) Suppose Alice shares a secret block cipher key, K_{AB} with Bob, and a different secret block cipher key, K_{AC} with Charlie. Describe a method for Alice to encrypt an m-block message (x_1,x_2, ...,x_m) such that it can only be decrypted with the cooperation of both Bob and Charlie. The ciphertext should only be a constant size greater than m blocks. You may assume that Bob and Charlie have a pre-established secret channel on which to communicate.

(b) Now, suppose Alice shares a block cipher key, K_{AB} with Bob, a block cipher key K_{AC} with Charlie, and a block cipher key K_{AD} with David. Describe a method for Alice to encrypt an m-block message such that any two of Bob, Charlie, and David can decrypt (for example, Bob and Charlie can decrypt), but none of them can decrypt the message themselves. Again, the ciphertext should only be a constant size greater than m blocks.
Hint: Pick a random message encryption key to encrypt the message with, then add ciphertext blocks to the ciphertext header.

(c) How does your solution from part (b) scale as we increase the number of recipients? In other words, suppose Alice has a secret key with each of n recipients and wants to encrypt so that any k out of n recipients can decrypt, but any k-1 cannot. What would be the length of the header as a function of n and k? Does it scale well?

5. Problem 2.10 in the textbook: We conduct a known-plaintext attack on an LFSR-based stream cipher. We know that the plaintext sent was:
1001 0010 0110 1101 1001 0010 0110
By tapping the channel we observe the following stream:
1011 1100 0011 0001 0010 1011 0001

1. What is the degree m of the key stream generator?
2. What is the initialization vector? (in the order z0 z1 z2)
3. Determine the feedback coefficients of the LFSR (in the order c0 c1 c2)
4. Draw a circuit diagram and verify the output sequence of the LFSR. If it starts with the initialization vector what would be its contents after 4 clock signals?

6. Problem 4.12 in the textbook: We now examine the gate (or bit) complexity of the MixColumn function, using the results from problem 4.11. We recall from the discussion of stream ciphers that a 2-input XOR gate performs a GF(2) addition.
1. How many 2-input XOR gates are required to perform one constant multiplication by 01, 02 and 03, respectively, in GF(2^8)?

2. What is the overall number of XOR gates that are required to complete one matrix–vector multiplication?

3. What is the number of XOR gates that are required for the entire Diffusion layer? (We assume permutations require no gates)

7. Problem 5.9 in the textbook: We are using AES in counter mode for encrypting a hard disk with 1 TB of capacity. What is the maximum length of the IV? 92 bits.

8. Problem 5.10 in the textbook: Sometimes error propagation is an issue when choosing a mode of operation in practice. In order to analyze the propagation of errors, let us assume a bit error (i.e., a substitution of a "0" by a "1" or vice versa) in a ciphertext block yi that corresponds to cleartext xi.

1. Assume an error occurs, during the transmission, in the ciphertext block yi. Which cleartext blocks are affected on Bob's side when using the ECB mode? List such blocks with a comma to separate any two (e.g., xi,xi+1,xi+2)

2. Again, assume block yi contains an error introduced during transmission. Which cleartext blocks are affected on Bob's side when using the CBC mode?

3. Suppose there is an error in the cleartext xi on Alice's side. Which cleartext blocks are affected on Bob's side when using the CBC mode?

4. Assume a single bit error occurs in the transmission of a ciphertext character in an 8-bit CFB mode. Which one of the following three statements is correct? (a) Only xi will be corrupted, (b) xi and a few additional blocks will be corrupted, (c) xi and all the consecutive blocks will be corrupted. Enter a or b or c.

9. Problem 1.4 from the textbook: Consider the relation between passwords and key size for a cryptosystem where the user enters a key in the form of a password.

1. Assume a password consisting of 8 letters, where each letter is encoded by the ASCII scheme (7 bits per character, i.e., 128 possible characters). What is the size of the key space which can be constructed by such passwords? Write the corresponding key length in bits?

2. Assume that most users use only the 26 lower-case letters from the alphabet instead of the full 7 bits of the ASCII-encoding. What is the corresponding key length in bits in this case?

3. At least how many characters are required for a password in order to generate a key length of 128 bits in case of letters consisting of
(a) 7-bit characters?

(b) 26 lowercase letters from the alphabet?