CSS322 – Quiz 3

Security and Cryptography, Semester 2, 2014

Prepared by Steven Gordon on 10 February 2015
css322y14s2q03, Steve/Courses/2014/s2/css322/assessment/quiz3.tex, r3556

Question 1 [2 marks]

Consider a mono-alphabetic cipher, with a selected mapping from plaintext to ciphertext for all possible plaintext values shown below (the mapping is split into two to fit it on the page).

```
p: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a
C: V W O Q R C P m f e g H q Z S t h F z r w Y c y D o -

p: b c d e f g h i j k l m n o p q r s t u v w x y z _ -
C: l L u _ E K s B A v n G N i T b k X p M j I U a J x d

p: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b
C: _ D g f i J T e z v w Q L G N d c b O ! l y R o M n H V

p: c d e f g h i j k l m n o p q r s t u v w x y z _ ! # ?
C: x Z k E j u q C p K r F h B A X I P Y ? t S W U # a s m
```

(a) With a computer that can make [10^{13} | 10^{10} | 10^{12} | 10^{11} | 10^{9}] decrypt attempts per second, what is the worst case time for a brute force attack? [2 marks]

Answer. *There were two variants of the mono-alphabetic cipher: one with 56 characters (26 uppercase, 26 lowercase, 4 other characters) and the other with 54 characters. A single mapping from the possible input plaintext characters to the corresponding ciphertext characters is given. This single mapping corresponds to using a key. A different mapping corresponds to a different key. How many possible keys are there? The number of possible keys is the number of possible mappings. With 56 (or 54) characters that must map to a unique character from that same set (i.e. only single alphabet, hence "mono-alphabetic"), there are 56! (or 54!) mappings. Therefore there are 56! (or 54!) possible keys. A brute force attack requires trying all possible keys. The time it takes depends on the number of keys and the speed at which a single key can be tried. At a rate of* 10^x *keys per second, a brute force attack on the cipher with 56 characters takes:*

$$\frac{56!}{10^x} \text{seconds}$$

Question 2 [3 marks]

(a) The process of converting a coded message back to the original message is called *decryption*.

(b) *Confidentiality* is a security service that ensures the contents of a message are not released to unauthorised people.

(c) In a *masquerade* attack, a malicious user pretends to be someone they are not.

(d) *Access control* is a security service that controls who can have access to a resource.

(e) The process of converting a coded message back to the original message is called *decryption*.

(f) In a *traffic analysis* attack, a malicious user observes patterns of communications, without having to read the message contents.

(g) *Authentication* is a security service that assures the received data originated from the claimed sender.

(h) In a *replay* attack, a malicious user sends an identical copy of a previous message they have intercepted.

(i) The information known only to sender and receiver in a cipher is called a*key*.

(j) In a *modification* attack, a malicious user changes the contents of an intercepted message.

(k) The process of converting an original message into a coded, apparently random message is called *encryption*.

(l) *Availability* is a security service that assures a system is always accessible to authorised users.

(m) In a *denial of service* attack, a malicious user overloads a server or network with traffic.

(n) *Data integrity* is a security service that assures data received are exactly as sent.

(o) The process of converting an original message into a coded, apparently random message is called *encryption*.

Question 3 [2 marks]

Consider the ciphertext [`seyosxisstuecixhra` | `cieaexshxettrbxass` | `fsxbosrrlteweixuco` | `sshxktoxeisxeorxdyot` | `sthseeteitaxabrdsenx`] output from a rows/columns transposition cipher using the key [`463152` | `164325` | `236451` | `53124` | `42135`]. What is the plaintext?

Plaintext: _____

Answer.

(a) *Plaintext:* `thiscourseiseasy`*; Key:* `463152`*;*
Ciphertext: `seyosxisstuecixhra`

(b) *Plaintext:* `caesaristhebest`*; Key:* `164325`*;*
Ciphertext: `cieaexshxettrbxass`

(c) *Plaintext:* `bruteforceisslow`*; Key:* `236451`*;*
Ciphertext: `fsxbosrrlteweixuco`

(d) *Plaintext:* `deskeyistooshort`*; Key:* `53124`*;*
Ciphertext: `sshxktoxeisxeorxdyot`

(e) *Plaintext:* `aesisbetterthandes`*; Key:* `42135`*;*
Ciphertext: `sthseeteitaxabrdsenx`

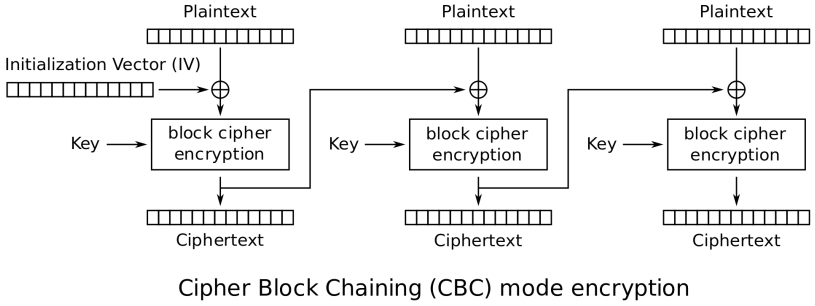

Figure 1: CBC encryption

Question 4 [2 marks]

Using block cipher *ABC* (the single version shown in the table), the plaintext [11010011 | 00101010 | 11010011 | 00101010 | 00101010] is encrypted using key [10 | 01 | 10 | 01 | 01] with CBC and IV [0110 | 0111 | 1110 | 1000 | 0111] (encryption with CBC is shown in Figure 1). What is the ciphertext? [3 marks]

Answer. *Split the plaintext into two 4-bit blocks then XOR the first block with the IV. The result is encrypted (lookup the ciphertext from the table), giving the first 4 bits of ciphertext. Then XOR the next 4-bits of plaintext with the previous ciphertext. The result is encrypted to give the last 4 bits of ciphertext.*

- *P: 1101 0011; IV=0110; K=10; C=1001 0000*
- *P: 0010 1010; IV=0111; K=01; C=1111 1111*
- *P: 1101 0011; IV=1110; K=10; C=1111 1010*
- *P: 0010 1010; IV=1000; K=01; C=0010 1011*

Question 5 [3 marks]

Consider a 4 bit block cipher, called *ABC*, that uses 2-bit keys. The ciphertext for all possible plaintexts and keys for cipher ABC are given below. To increase the strength of ABC against brute-force attack, I will apply the algorithm twice using a 4-bit key, K, which is two independent keys from ABC. The resulting cipher is *Double-ABC*. I have chosen a key and sent multiple ciphertexts to my friend. You are an attacker that has discovered two pairs of (plaintext, ciphertext): [(0111,1101) and (1101,0100) | (0000,0101) and (1111,0011) | (0111,1101) and (1101,0100) | (0000,0101) and (1111,0011) | (0111,1101) and (1101,0100)]. Use a meet-in-the-middle attack to determine the most likely key I used. Show the steps.

Plaintext	00	01	10	11		Plaintext	00	01	10	11
0000	0001	0101	1000	0111		1000	1000	1011	0101	1000
0001	1101	0111	1101	0101		1001	1100	0000	0010	0110
0010	0000	0110	0111	1010		1010	1010	0010	0000	0100
0011	0101	1101	1111	0011		1011	1011	1100	1001	1001
0100	0111	1000	1100	1101		1100	0110	0011	1010	1100
0101	1001	1111	1011	0001		1101	1111	1110	0100	0000
0110	0011	1001	0001	1011		1110	0100	0100	0011	0010
0111	1110	0001	0110	1111		1111	0010	1010	1110	1110

Answer. *Consider for the given pair (0111, 1101) and (1101, 1110).*

Using the pair (0111, 1101) apply a 2-bit brute force on the plaintext 0111 to get:

$K = 00, P = 0111, X_{1,1} = 1110$

$K = 01, P = 0111, X_{1,2} = 0001$

$K = 10, P = 0111, X_{1,3} = 0110$

$K = 11, P = 0111, X_{1,4} = 1111$

Now decrypt the ciphertext 1101 with all possible keys:

$K = 00, C = 1101, X_{2,1} = 0001$

$K = 01, C = 1101, X_{2,2} = 0011$

$K = 10, C = 1101, X_{2,3} = 0001$

$K = 11, C = 1101, X_{2,4} = 0100$

We note that there are two pairs of X that match:

(a) $X_{1,2} = X_{2,1}$ *giving a possible key 0100*

(b) $X_{1,2} = x_{2,3}$ *giving a possible key 0110*

So now try key 0100 with the next pair (1101,0100):

$P = 1101, K = 01, X = 1110, K = 00, C = 0100$

Since the key works for this pair we can assume this is the correct key. You could confirm by encrypting 1101 with the other key (0110) and you will see that the ciphertext 0100 is not *obtained. The correct key is 0100.*

Consider for the given pair (0000, 0101) and (1111, 0011).

Using the pair (0000, 0101) apply a 2-bit brute force on the plaintext 0000 to get:

$K = 00, P = 0000, X_{1,1} = 0001$

$K = 01, P = 0000, X_{1,2} = 0101$

$K = 10, P = 0000, X_{1,3} = 1000$

$K = 11, P = 0000, X_{1,4} = 0111$
Now decrypt the ciphertext 0101 with all possible keys:
$K = 00, C = 0101, X_{2,1} = 0011$
$K = 01, C = 0101, X_{2,2} = 0000$
$K = 10, C = 0101, X_{2,3} = 1000$
$K = 11, C = 0101, X_{2,4} = 0001$
We note that there are two pairs of X that match:

(a) $X_{1,1} = X_{2,4}$ *giving a possible key 0011*

(b) $X_{1,3} = x_{2,3}$ *giving a possible key 1010*

So now try key 0011 with the next pair (1111,0011):
$P = 1111, K = 00, X = 0010, K = 11, C = 0101$
The ciphertext doesn't match the expected value. So this is the wrong key. Lets try the next possible key 1010:
$P = 1111, K = 10, X = 1110, K = 10, C = 0011$
The ciphertext matches so the key 1010 is the correct key.