

# CSS322 – Quiz 1

Security and Cryptography, Semester 2, 2011

Prepared by Steven Gordon on 21 January 2012

CSS322Y11S2Q01, Steve/Courses/2011/S2/CSS322/Assessment/Quiz1.tex, r2117

For reference, you may use the following mapping of English characters to numbers:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

## Question 1 [3 marks]

Consider the ciphertext [ ytoærrstssexauicuiræohræecæ | itæsræioiæhoettærisctæ | htæssøatætsææmeøæubæxiihnyqnvoæ | tgnhogitæktæyæwøærxniæiuø ] output from a rows/columns transposition cipher using the key [ 4271653 | 541632 | 3162745 | 81237456 ]. What is the plaintext?

**Answer.**

- (a) *Plaintext: areyousurethisiscorrect; Key: 4271653;*  
*Ciphertext: ytoærrstssexauicuiræohræecæ*
- (b) *Plaintext: thisisnotcorrectisit; Key: 541632;*  
*Ciphertext: itæsræioiæhoettærisctæ*
- (c) *Plaintext: thisquestionmusthavebeentooeasy; Key: 3162745;*  
*Ciphertext: htæssøatætsææmeøæubæxiihnyqnvoæ*
- (d) *Plaintext: ithinkyougotitwrong; Key: 81237456;*  
*Ciphertext: tgnhogitæktæyæwøærxniæiuø*

## Question 2 [3 marks]

- (a) Name an attack that the [ data integrity | authentication | availability | data confidentiality ] service aims to prevent. Describe how the attack works.

**Answer.**

- i. *Data integrity aims to prevent a modification attack. In this attack a malicious user intercepts a message before it reaches the destination, then modifies the message and forwards the modified message to the destination. The destination thinks that the received (modified) message was originally sent by the source.*
- ii. *Authentication service aims to provide a masquerade attack. In this attack a malicious user sends a message, pretending to be someone else. When the destination receives the message they think it came from the “someone else”, not the malicious user.*

- iii. *Availability service aims to prevent a denial of service attack. In this attack a malicious user sends a large amount of network traffic to a server such that the server (or connection to it) is overloaded. The server is then unavailable for normal users.*
- iv. *Data confidentiality aims to prevent release of the message contents. In this attack a malicious user intercepts a message and obtains the contents of that message.*

(b) Explain the difference between a passive and active attack.

**Answer.** *A passive active does not modify the system resources, whereas an active attack does. Consider the system (set of users, message sent) in the absence of a passive attack. Now consider the system in the presenve of a passive active. In both cases the system is the same: each user sends/receives same set of messages. Now compare the system in the absence and presence of an active attack. When an active attack is present the set of messages sent/received by users (or the messages themselves) are different from when the attack is absent.*

### Question 3 [4 marks]

Consider a Vigenère cipher where the alphabet is the first ten letters from the English alphabet, i.e. *a* to *j*.

- (a) Encrypt the plaintext [ *died* | *dice* | *high* | *hide* ] with keyword *bed*. What is the ciphertext?

**Answer.**

- i. *Plaintext: died; Keyword: bed;*  
*Ciphertext: eche*
- ii. *Plaintext: dice; Keyword: bed;*  
*Ciphertext: ecff*
- iii. *Plaintext: high; Keyword: bed;*  
*Ciphertext: icji*
- iv. *Plaintext: hide; Keyword: bed;*  
*Ciphertext: icgf*

*The keyword **bed** is equivalent to:*

*1 4 3*

*Note that since the plaintext is four characters the key becomes:*

*1 4 3 1*

*The plaintext **died** is equivalent to:*

*3 8 4 3*

Now apply the Caesar cipher (but mod 10):

3 8 4 3

1 4 3 1

4 2 7 4

e c h e

Gives the ciphertext *eidg*.

Using plaintext *dice*:

3 8 2 4

1 4 3 1

4 2 5 5

e c f f

Using plaintext *high*:

7 8 6 7

1 4 3 1

8 2 9 8

i c j i

Using plaintext *hide*:

7 8 3 4

1 4 3 1

8 2 6 5

i c g f

- (b) If a computer took 1ms to perform one decryption, on average how long would a brute force attack take on this cipher?

**Answer.** The keyword in this case is 3 letters, but the attacker doesn't know this. They know the plaintext is 4 letters and that the key must be as long as the plaintext, so must try all combinations of 4 letters for the key (note the keyword is what is chosen by the user; the key is generated from the keyword and used for encryption). Each letter can be one of 10 choices. So there are  $10 \times 10 \times 10 \times 10$  possible keys to try. At a rate of 1 per 1ms, 10,000 attempts would take 10 seconds. But on average the attacker would need half as many attempts. So it will take 5 seconds.