# CSS322 – Quiz 1

Security and Cryptography, Semester 2, 2012

Prepared by Steven Gordon on 25 November 2012
CSS322Y12S2Q01, Steve/Courses/2012/s2/css322/assessment/quiz1.tex, r2575

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 [2 marks]

Encrypt the first 3 letters of your firstname using the Vigenère cipher with the keyword *hello*.

**Answer.** *Find the first three letters of your firstname in the list below; the second three letters is the ciphertext. These values were obtained using* `crypto`.

*jin qmy; tim amx; nit ume; usa bwl; nat uee; say zej; ali hpt; tha all; wip dma; saw zeh; cho jlz; the alp; jak qev; pav weg; pic wmn; kra rvl; nap uea; anu hrf; rav yeg; tan aey; att hxe; akk hov; tan aey; war dec; nat uee; pra wvl; por wsc; sal zew; ara hvl; tha all; taw aeh; lal sew; kit rme; dan key; nat uee; thi alt; sup zya; wir dmc; kan rey; cha jll; nat uee; tan aey;*

## Question 2 [5 marks]

Fill in the blanks.

(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) Consider a One Time Pad that uses hexadecimal (base-16) digits, as opposed to English letters. A computer system can decrypt this One Time Pad at a rate of $10^6$ messages per second. In theory, the average time to apply a brute force attack on this One Time Pad when a message is 100 characters is $16^{100}/10^6/2$ seconds. [2 marks]

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

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

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

(h) Consider a One Time Pad that uses hexadecimal (base-16) digits, as opposed to English letters. A computer system can decrypt this One Time Pad at a rate of $10^9$ messages per second. In theory, the average time to apply a brute force attack on this One Time Pad when a message is 200 characters is $16^{200}/10^9/2$ seconds. [2 marks]

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

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

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

(l) Consider a One Time Pad that uses octal (base-8) digits, as opposed to English letters. A computer system can decrypt this One Time Pad at a rate of $10^8$ messages per second. In theory, the average time to apply a brute force attack on this One Time Pad when a message is 100 characters is $8^{100}/10^8/2$ seconds. [2 marks]

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

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

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

(p) Consider a One Time Pad that uses octal (base-8) digits, as opposed to English letters. A computer system can decrypt this One Time Pad at a rate of $10^6$ messages per second. In theory, the average time to apply a brute force attack on this One Time Pad when a message is 300 characters is $8^{300}/10^6/2$ seconds. [2 marks]

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

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

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

(t) Consider a One Time Pad that uses octal (base-8) digits, as opposed to English letters. A computer system can decrypt this One Time Pad at a rate of $10^7$ messages per second. In theory, the average time to apply a brute force attack on this One Time Pad when a message is 200 characters is $8^{200}/10^7/2$ seconds. [2 marks]

**Answer.** *An explanation of the last part using octal (base-8) as an example. The characters available for the plaintext are: 0, 1, 2, 3, 4, 5, 6, 7. There are 8 values (if using hexadecimal, then there are 16 values). With a one time pad, as seen in the lecture, each letter in the message is encrypted using a Caesar cipher. Since there are 8 plaintext values then there are also 8 possible values of k in the Caesar cipher: 0 through to 7. In the one time pad the keyword is as long as the message and random. So how many possible keys are available with a 200 character message? For the 1st character of plaintext, there are 8 possible Caesar keys; for the 2nd character of plaintext, there are 8 possible Caesar keys; . . . ; for the 200th character of plaintext, there are 8 possible Caesar keys. So in total, there are* $8^{200}$ *possible keys. A brute force attack requires trying all possible keys. Decrypting at a rate of* $10^7$ *messages per second, then the maximum time a brute force attack is* $8^{200}/10^7$ *seconds. But that is only for the case when the key is the last one we try. Some times we will have to try few keys, and other times many keys. On average, half of the keys must be tried before a match is found. So the average time for the brute force attack is* $8^{200}/10^7/2$ *seconds.*

## Question 3 [3 marks]

Consider the ciphertext [ `atxevxnsxmiemexysx` | `tvsiexsyxirxsaxhey` | `nmxrdnocsslxauxwox` | `izssiyhiaqsxtue` | `arsxliaxyiixpaerfsex`] output from a rows/columns transposition cipher using the key [ `463152` | `164325` | `236451` | `53124` | `42135`]. What is the plaintext?

**Answer.**

(a) *Plaintext:* `mynameissteve`*; Key:* `463152`*;*
*Ciphertext:* `atxevxnsxmiemexysx`

(b) *Plaintext:* `thisisveryeasy`*; Key:* `164325`*;*
*Ciphertext:* `tvsiexsyxirxsaxhey`

(c) *Plaintext:* `rowsandcolumns`*; Key:* `236451`*;*
*Ciphertext:* `nmxrdnocsslxauxwox`

(d) *Plaintext:* `thisquiziseasy`*; Key:* `53124`*;*
*Ciphertext:* `izssiyhiaqsxtue`

(e) *Plaintext:* `playfairiseasier`*; Key:* `42135`*;*
*Ciphertext:* `arsxliaxyiixpaerfsex`