CSS322 – Quiz 2

Security and Cryptography, Semester 2, 2013

Prepared by Steven Gordon on 28 November 2013
css322y13s2q02, Steve/Courses/2013/s2/css322/assessment/quiz2.tex, r3015

Question 1 [2.5 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? [1.5 mark]

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:*

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

(b) Explain a practical attack against the cipher. [1 mark]

Answer. *Despite having too many keys to make a brute force attack impossible, a more intelligent attack on a monoalphabetic cipher is practically possible. Since each plaintext letter will always map to the same ciphertext letter when using a particular key, the frequency of letters (digrams, trigrams, words) on the plaintext will be reflected also in the ciphertext. Therefore with a long ciphertext, by counting letters (digrams, trigrams, words), an attacker can esitmate the most likely input plaintext letters (digrams, trigrams, words) that they correspond to. To see an example of such an attack see: http://sandilands.info/sgordon/classical-ciphers-frequency-analysis-examples*

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]

Using the first 8 letters of your full name (convert all uppercase to lowercase, and delete any characters which are not letters a—z) as a keywords, encrypt the **Error in quiz: originally it said ciphertext, but should be plaintext** plaintext [*comma* | *muddy* | *polls* | *sunny* | *merry*] using the Playfair cipher.

Error in quiz: I wanted you to write your name/keyword here, not plaintext Keyword: _____

Ciphertext: _____

Answer. *An example using my name (stevengo) and the plaintext comma. Create the Playfair matrix:*

s t e v n
g o a b c
d f h i k
l m p q r
u w x y z

The plaintext needs to be broken into pairs, with the exception that the two "m"'s must be split by a special character "x": co mx ma. Now lookup the pairs in the matrix to find the ciphertext (see lectures for details). The ciphertext is: gapwpo.

Question 4 [2.5 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`