CSS322 – Quiz 1

Security and Cryptography, Semester 2, 2010

Prepared by Steven Gordon on 19 November 2010
CSS322Y10S2Q01, Steve/Courses/CSS322/Assessment/Quiz1.tex, r1525

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 [4 marks]

You have access to a computer that can perform [10^{12} | 10^{15} | 10^{10} | 10^{10} | 10^{12} | 10^{15}] decryption operations every second. What is the average time it would take you to find the plaintext for a given ciphertext when using the following cipher: [Monoalphabetic substitution cipher | Vigenère cipher with 10 letter keyword | Playfair cipher | Monoalphabetic substitution cipher | Vigenère cipher with 8 letter keyword | Playfair cipher]. Assume each cipher uses the 26 letters from the English alphabet (although keywords, if used, also use these letters, they do not have to be a known English word or phrase). Assume each decryption operation also includes a check as to whether the plaintext is correct or not (and such a check always works).

Answer. *With the monoalphabetic cipher the key is a mapping from one letter in the alphabet to another available letter in the alphabet. For example, the first letter can map to any of the 26 letters; the second letter can map to any of the other 25 letters; the third to any of the other 24 letters; and so on. Hence there are* $26 \times 25 \times 24 \times \ldots \times 2 \times 1 = 26!$ *possible mappings or keys. (Alternatively, with* 26 *letters, there are* 26! *ways to arrange those letters).*

With a Playfair cipher the keyword is chosen by the user. The maximum length is 25 letters (since the Playfair matrix is 5×5*). Each letter in the alphabet can only occur once in the matrix and hence, with* 25 *letters there are* 25! *ways to arrange those letters.*

With the Vigeneère cipher a keyword of 10 letters allows for 26^{10} *possible keywords. This is because each letter of the keyword can be any one of the 26 letters from the alphabet.*

Knowing the number of possible keys (i.e. the key space), one average a brute force attack needs to search half *of the key space to find the correct plaintext. Hence the time to find the ciphertext is:*

(a) Monoalphabetic, 10^{12}*:* $\frac{26!}{10^{12}} \times \frac{1}{2}$

(b) Vigenère, 10^{15}*:* $\frac{26^{10}}{10^{15}} \times \frac{1}{2}$

(c) Playfair, 10^{10}*:* $\frac{25!}{10^{10}} \times \frac{1}{2}$

(d) Monoalphabetic, 10^{10}*:* $\frac{26!}{10^{10}} \times \frac{1}{2}$

(e) Vigenère, 10^{12}*:* $\frac{26^8}{10^{12}} \times \frac{1}{2}$

(f) Playfair, 10^{15}*:* $\frac{25!}{10^{15}} \times \frac{1}{2}$

Question 2 [2 marks]

What is the main reason a polyalphabetic cipher (such as Vigenère) offers stronger security than a monoalphabetic substitution cipher?

Answer. *In a monoalphabetic cipher, each instance of a single input element is always transformed into the same output element (when using the key). This makes frequency analysis based on the language structure easy. E.g. in English texts, you may expect 12% of letters to be* e. *Therefore in the ciphertext if a letter makes up 12% of all letters, then it is likely to correspond to the plaintext letter* e. *In a polyalphabetic cipher each instance of the same element in the input can become different elements in the output. This makes cryptanalysis harder, as the frequency of letters in the ciphertext no longer matches the frequency of letters in the plaintext.*

Question 3 [4 marks]

Encrypt the plaintext `steven` with a [Playfair cipher | One-time pad | Vigenère cipher | Vigenère cipher | Playfair cipher | One-time pad] using the keyword [`crypto` | `xfqbjs` | `secure` | `crypto` | `secure` | `qopegk`].

Answer. *The ciphertext should be (see below for detailed steps):*

(a) Playfair, `crypto`*: ZEAZBS*

(b) One-time pad, `xfqbjs`*: PYUWNF*

(c) Vigenère, `secure`*: KXGPVR*

(d) Vigenère, `crypto`*: UKCKXB*

(e) Playfair, `secure`*: RNSWSO*

(f) One-time pad, `qopegk`*: IHTZKX*

Playfair matrix with keyword `crypto`*:*
`c r y p t`
`o a b d e`
`f g h i k`
`l m n q s`
`u v w x z`
Encrypting pairs of plaintext: `st` $\rightarrow$ *ZE,* `ev` $\rightarrow$ *AZ,* `en` $\rightarrow$ *BS.*
For the one-time pad and Vigenère ciphers, treat the letters as numbers an apply the Caesar cipher using an appropriate key.
One-time pad with keyword `xfqbjs`*:*
`s t e v e n`
18 19 04 21 04 13
`x f q b j s`
23 05 16 01 09 18
Sum the plaintext number and keyword number:

41 24 20 22 13 31
Modulo 26:
15 24 20 22 13 05
Produces the letters: `PYUWNF`.
Vigenère with keyword `secure`*:*
`s t e v e n`
18 19 04 21 04 13
`s e c u r e`
18 04 02 20 17 04
Sum the plaintext number and keyword number:
36 23 06 41 21 17
Modulo 26:
10 23 06 15 21 17
Produces the letters: `KXGPVR`.
Vigenère with keyword `crypto`*:*
`s t e v e n`
18 19 04 21 04 13
`c r y p t o`
02 17 24 15 19 14
Sum the plaintext number and keyword number:
20 36 28 36 23 27
Modulo 26:
20 10 02 10 23 01
Produces the letters: `UKCKXB`.
Playfair matrix with keyword `secure`*:*
`s e c u r`
`a b d f g`
`h i k l m`
`n o p q t`
`v w x y z`
Encrypting pairs of plaintext: `st` $\rightarrow$ `RN`, `ev` $\rightarrow$ `SW`, `en` $\rightarrow$ `SO`.
One-time pad with keyword `qopegk`*:*
`s t e v e n`
18 19 04 21 04 13
`q o p e g k`
16 14 15 04 06 10
Sum the plaintext number and keyword number:
34 33 19 25 10 23
Modulo 26:
08 07 19 25 10 23
Produces the letters: `IHTZKX`.