FIT1047 Tutorial 7

Topics

- Classical cryptography, Cryptool
- Ciphers: CAESAR and Monoalphabetic; RSA

Instructions

- The tasks are supposed to be done in groups.
- Task 0 should be done before your tutorial.

Task 0: Cryptool Online

In this task you get to know Cryptool, a learning tool for cryptography. We use the online version at http://www.cryptool-online.org/. This version mainly supports classical ciphers up to after the second world war. Ciphers can directly be tested.
For learning about modern cryptography, the full version of the tool for Windows can be downloaded here: https://www.cryptool.org/

0.a Load Cryptool online at http://www.cryptool-online.org/, read the text on the initial page and then chose *Ciphers* in the top menu.

0.b Read the text on Ciphers and then chose the Monoalphabetic Substitution Cipher.

   (a) Read the text on the Monoalphabetic substitution cipher. Click on *test it* and create your own cipher alphabet. Then test a message. Look at which part of the Ciphertext changes when you just change one letter in the plaintext, or one word in the plaintext.

   (b) Then read the descriptions for the Caesar cipher and the Polybius cipher. Why can the Polybius cipher be considered more secure. Why is it still a very insecure cipher?

Task 1: Decryption exercise

The following ciphertext is derived from an English plaintext using a Monoalphabetic Substitution Cipher. It is not case sensitive, “,” and “.” are unencrypted, blanks are not deleted:

```
wy wj s &szi ywdq mlz y*q
zqtqaawlb. say*lvk* y*q
&qsy* jysz *sj tqqb &qjyzlgq&,
wd{qzwsa yzll{j *suq &zwuqb y*q
zqtqa mlzoqj mzld y*qwz *w&&qb
tsjq sb& {vzjvq& y*qd sozljj y*q ksashg.

qus&wbk y*q &zqs&q& wd{qzwsa jyszmaqqy,
s kzlv{ lm mzqq&ld mwk*yqzj aq& tg
aviq jigrsaiqz *sj qjystawj*q& s
bqr jqozqy tsjq lb y*q zqdlyq
woq rlza& lm *ly*.
```

1.a Which approach would you chose to start an analysis of this ciphertext?

1.b What is the plaintext?

1.c Which key is used?

Hint: There are some hints in the text on Monoalphabetic Substitution Ciphers and you can use Cryptool to try your guesses. In the tool, in the Ciphertext-aphabet box, you can type in your guesses. First use one character that does not appear in the ciphertext as placeholder for all letters (i.e. the plaintext alphabet is 26 characters long, thus just fill the box with 26 times the same character). Then exchange this placeholder step-by-step with the guesses for single characters.

Task 2: RSA using pencil and paper

The public-key algorithm RSA is based on *modular exponentiation*. The expression $a^b mod n$ means that instead of calculating a^b, the result of a^b is divided by n and the result is just the remainder.

Example: $4^2 mod 7 = 2$ because $4^2 = 16$ and the remainder of 16 divided by 7 is 2.
A guy called Serge Matovic has written a short example for RSA just using small numbers:
http://sergematovic.tripod.com/rsa1.html
In principle, it can be done just using pencil and paper (for some steps a calculator is useful...)

2.1 Read the text. What is the server's secret key and what is the sever's public key.

2.2 Calculate encryption and decryption with message P=13.