Track A
INFA723 Homework 1

The homework assignment will be graded based on the following criteria:

- Accuracy: 1) the solution meets specific requirements in the problem description; 2) the solution produces correct results; 2) the procedures adopted in the solution are technically sound.
- Efficiency: efficiency will be one of the criteria when grading programing assignment. The solution should produce the desired results efficiently.
- Effort/neatness: the solution includes excellent effort, and all relate work is shown neatly and organized well.

Homework assignment feedback will be available through the DropBox folder on D2L.

1. (10 points) CrypTool (http://www.cryptool.org/) is a free, open-source e-learning application, used worldwide in the implementation and analysis of cryptographic algorithms. The current version offers the following highlights:

- Numerous classic and modern cryptographic algorithms (encryption and decryption, key generation, secure passwords, authentication, secure protocols, etc.)
- Visualization of several algorithms (Caesar, Enigma, RSA, Diffie-Hellman, digital signatures, AES, etc.)
- Cryptanalysis of several algorithms (Vigenère, RSA, AES, etc.)
- Cryptanalytical measurement methods (entropy, n-grams, autocorrelation, etc.)
- Related auxiliary methods (primality tests, factorization, base64 encoding, etc.)
- Number theory tutorial
- Comprehensive online help
- Accompanying script with additional information about cryptology
- And plenty more!

The program works in Win32 environment and can be downloaded at

http://www.cryptool.org/index.php/en/download-topmenu-63.html.

We will use this tool for many class assignments.

a) Download CryptTool (v1.4.42) and install it on your computer.
b) Encrypt the following message

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable. —The Art of War, Sun Tzu

using Caesar Cipher (Shift-3, C=(p+3) mod 26) and submit your cipher text.

c) Decrypt the following message

Lw'v hdvb wr xvh!

using Casear Cipher (Shift-3, C=(p+3) mod 26) and submit your plaintext.

2. (15 points) List and briefly define the six security services as defined in the OSI security architecture.

3. (15 points) The following cipher text was generated using a simple substitution algorithm.

Nbkyrpsrws jifx. Jir kjqqbofr mssmne tiarp syrqr nbpntgqsminrq bq syr optsr-cjpnr mkkpjmny jc spxbih mff kjqqbofr erxq. Bc syr erx qkmnr bq urpx fmphr, sybq ornjgrq bgkpmnsbnmf. Sytq, syr jkkjiris gtqs prfx ji mi mimfxqbq jc syr nbkyrpsrws bsqrfc, hrirpmffx mkkfxbih umpbjtq qsmsbqsbnmf srqsq sj bs. Eijvi kfmbisrws. Syr mimfxqs gmx or mofr sj nmkstpr jir jp gjpr kfmbisrws grqqmhrq mq vrff mq syrbp rinpxksbjiq. Vbsy sybq eijvfrahr, syr mimfxqs gmx or mofr sj aratnr syr erx ji syr omqbq jc syr vmx bi vybny syr eijvi kfmbisrws bq spmiqcjpgra. Nyjqri kfmbisrws. Bc syr mimfxqs bq mofr sj nyjjqr syr grqqmhrq sj rinpxks, syr mimfxqs gmx arfborpmsrfx kbne kmssrpiq syms nmi or rwkrnsra sj prurmf syr qsptnstpr jc syr erx.

Decrypt the message using Cryptool (Hint: combine with manual analysis).

4. (15 points) Given a 5x5 matrix for Playfair cipher

a. How many possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Express your answer as an approximate power of 2.
b. Now take into account the fact that some Playfair keys produce the same encryption results. How many effectively unique keys does the Playfair cipher have?

5. (15 points) When the PT-109 American patrol boat, under the command of Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, a message was received at an Australian wireless station in Playfair code:

KXJEY UREBE ZWEHE WRYTU HEYFS
KREHE GOYFI WTTTU OLKSY CAJPO
BOTEI ZONTX BYBNT GONEY CUZWR
GDSON SXBOU YWRHE BAAHY USEDQ

The key used was *royal new zealand navy*. Decrypt the message using Cryptool. Translate TT into tt.

6. (15 points) Using the Vigenere cipher, encrypt the world “explanation” using the key *leg*.

7. (15 points) Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. Detailed discussions about Meltdown and Spectre can be found at

https://meltdownattack.com/

Choose either one of the attacks. Read the paper posted in the website and answer the following questions.

a) Briefly describe the attack and the hardware vulnerabilities which make the attack possible.
b) What is the general impact of the attack to computer security?
c) What can we do to mitigate the security risks due to the attack?

The answers should be based on the attack you choose to study. You do not need to cover both attacks.