Homework 1

Track A

1. CrypTool (10 points)
   1. Download CryptTool (v1.4.42) and install it on your computer.

A screenshot of a computer

Description automatically generated

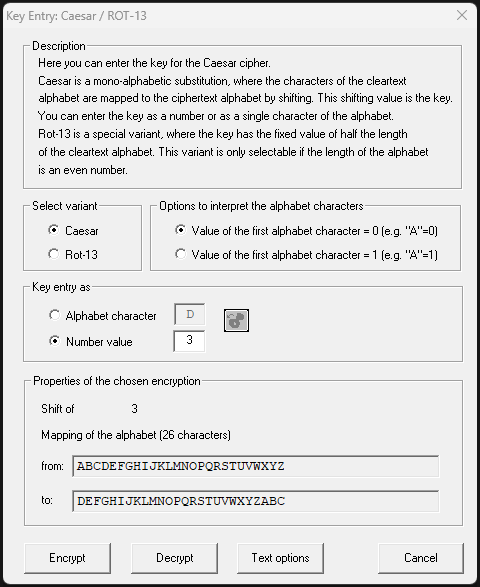
* 1. Encrypt the following message using Caesar Cipher (Shift-3, C=(p+3) mod 26) and submit your ciphertext

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

A screenshot of a chat

Description automatically generated

* + 1. Wkh duw ri zdu whdfkhv xv wr uhob qrw rq wkh olnholkrrg ri wkh hqhpb'v qrw frplqj, exw rq rxu rzq uhdglqhvv wr uhfhlyh klp; qrw rq wkh fkdqfh ri klv qrw dwwdfnlqj, exw udwkhu rq wkh idfw wkdw zh kdyh pdgh rxu srvlwlrq xqdvvdlodeoh. —Wkh Duw ri Zdu, Vxq Wcx

1. Security Services (15 points) : List and briefly define the six security services as defined in the OSI security architecture
   1. Authentication : assure the recipient that the message is from the source that it claims to be from
      1. Peer entity authentication: Used in association with a logical connection to
      2. provide confidence in the identity of the entities connected.
      3. Data origin authentication: In a connectionless transfer, provides assurance that the source of received data is as claimed.
   2. Access Control: ability to limit and control the access to host systems and applications via communications links.
   3. Data Confidentiality: the protection of transmitted data from passive attacks and the protection of transmitted data from passive attacks.
   4. Data Integrity: assures that messages are received as sent with no duplication, destruction, insertion, modification, reordering, or replays
   5. Nonrepudiation: prevents either sender or receiver from denying a transmitted message.
   6. Availability Service: a system resource being accessible and usable upon demand by an authorized system entity
2. Simple Substitution Cipher (15 points)
   1. Decrypt the provided ciphertext using Cryptool (Hint: combine with manual analysis)
      1. Analyzed n-grams
         1. Compared to <http://practicalcryptography.com/cryptanalysis/>
   2. Ciphertext only. One possible attack under these circumstances is the brute-force approach of trying all possible keys. If the key space is very large, this becomes impractical. Thus, the opponent must rely on an analysis of the ciphertext itself, generally applying various statistical tests to it. Known plaintext. The analyst may be able to capture one or more plaintext messages as well as their encryptions. With this knowledge, the analyst may be able to deduce the key on the basis of the way in which the known plaintext is transformed. Chosen plaintext. If the analyst is able to choose the messages to encrypt, the analyst may deliberately pick patterns that can be expected to reveal the structure of the key. deduce the key on the basis of the way in which the known plaintext is transformed.
3. Playfair Cipher (15 points)
   * Given a 5x5 matrix for the Playfair cipher:
   * Calculate the possible keys the Playfair cipher can have (ignore identical encryption results). Express your answer as an approximate power of 2.
   * Consider identical encryption results. How many effectively unique keys does the Playfair cipher have?