# Homework 1

Track A

## CrypTool (10 points)

* 1. Download CryptTool (v1.4.42) and install it on your computer.

A screenshot of a computer

Description automatically generated

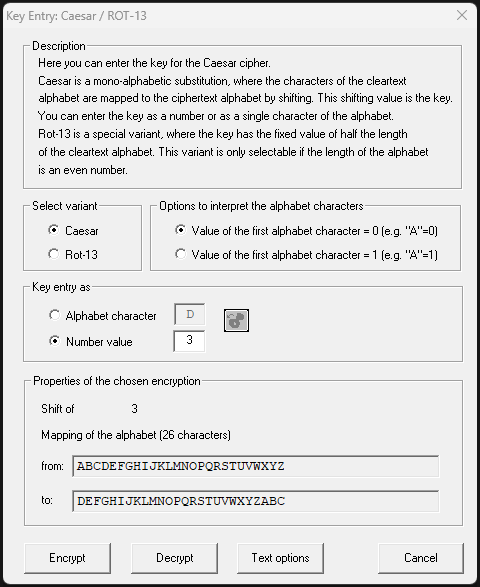
* 1. Encrypt the following message using Caesar Cipher (Shift-3, C=(p+3) mod 26) and submit your ciphertext

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

## 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

## 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.

## 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.

In a Playfair Cipher key, each letter of the alphabet, excluding 'J' which is usually combined with 'I', is placed in the matrix exactly once. Since the first letter can be chosen from 25 possibilities, the second letter from 24, and so on, the total number of unique keys that can be generated for the cipher is 25! Or 2^83.68

2^(x) = y

Log2(y) = x

25! = 15511210043330985984000000 (1.5511210043330985984 × 10^25)

Log2(15511210043330985984000000) = 83.6815

2^ 83.68 = (1.54949 × 10^25)

* + Consider identical encryption results. How many effectively unique keys does the Playfair cipher have?

In the Playfair Cipher, certain keys produce identical encryption results due to the symmetry of the matrix. In other words, shifting x rows or columns in would not change the encryption result. For example, the following rows shifts would produce the same result:

ABCDE

FGHIK

LMNOP

QRSTU

VWXYZ

--

EABCD

KFGHI

PLMNO

UQRST

ZVWXY

--

DEABC

IKFGH

OPLMN

TUQRS

YZVWX

--

CDEAB

HIKFG

NOPLM

STUQR

XYZVW

--

BCDEA

GHIKF

MNOPL

RSTUQ

WXYZV

--

[screenshot of cryptool here]

Then, for each of these 5 row shifts, there are 5 column shifts as well.

ABCDE

FGHIK

LMNOP

QRSTU

VWXYZ

--

FGHIK

LMNOP

QRSTU

VWXYZ

ABCDE

--

LMNOP

QRSTU

VWXYZ

ABCDE

FGHIK

--

QRSTU

VWXYZ

ABCDE

FGHIK

LMNOP

==

VWXYZ

ABCDE

FGHIK

LMNOP

QRSTU

---

etc

Since there are 5 rows and 5 columns in a 5x5 matrix, there are 5x5=25 equivalent matrices. Therefore, we can solve for the number of effectively unique keys (K) does that Playfair cipher has by doing the following:

K = total number of unique keys/ equivalent matrices

K = (25!)/25

K = 1\*2\*3\*4\*5 … 23\*24\*25 / 25

K = 1\*2\*3\*4\*5 … 23\*24

K = 24!

K = 24!

K = 6.20448e23

## PT-109 Message Decryption (15 points)

* When the PT-109 American patrol boat, commanded by Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, an encrypted message was received at an Australian wireless station in Playfair code. The message was encrypted using the key royal new zealand navy. Decrypt the message using Cryptool, and remember to translate TT into tt.

A screenshot of a computer

Description automatically generated

“PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKESUSU STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY INFORMATION X”

Convert tt to TT we get:

“PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKE**TT** STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY INFORMATION X”

## Vigenere Cipher (15 points)

Encrypt the word "explanation" using the key "leg"

pbvwetlxozr

A screenshot of a computer

Description automatically generated

## Meltdown and Spectre (15 points)

Choose either Meltdown or Spectre attack, study the paper posted on the website, and answer the following questions:

1. Briefly describe the attack and the hardware vulnerabilities that make the attack possible.
   1. Meltdown is a hardware vulnerability related to out-of-order execution. Out-of-order execution is a technique used by modern processors to improve performance by executing instructions non-sequentially. In order to maximize resources, the CPU uses Speculative Execution to predict upcoming instructions and attempts to assign them to execution units that are currently idle. However, in some cases, the CPU may encounter instructions that fetch data from privileged memory addresses. When this data is accessed from memory, a copy of it is stored in the cache for faster access in the future. The problem arises because, during speculative execution, the CPU may load data into this cache even before it is certain that the data will be needed. This means that even if the speculative execution is later discarded due to a privilege violation, the data may still remain in the cache. An attacker can exploit timing discrepancies in speculative execution and cache behavior using a cache side-channel attack such as Flush+Reload. By carefully timing and monitoring the cache accesses, the attacker can infer the contents of the privileged memory addresses and access sensitive data.
2. Discuss the general impact of the attack on computer security.
   1. The Meltdown attack has had a significant impact on computer security, as it challenges the current perspective on conventional hardware optimizations. While many of these optimization techniques that manipulate microarchitectural elements, such as execution units, registers, and cache memory, have existed for decades, their associated risks considered manageable. However, the granularity of Meltdown highlights the severity of these vulnerabilities as more than just minor flaws but rather critical security risks. Unlike previous vulnerabilities that target larger blocks of data, Meltdown allows attackers to access individual bits. This is particularly dangerous because it enables precise and targeted extraction of sensitive information. With access to individual bits, attackers can extract highly sensitive data including critical system secrets, passwords, and other sensitive data.
3. Explain mitigation strategies to mitigate the security risks due to the attack.
   1. As computers continue to evolve, there becomes an urgent need to redesign CPUs to better isolate and protect privileged memory and minimize the impact of speculative execution on security. This need stems from the recognition that even software explicitly designed to defend against side-channel attacks may not be sufficient if the hardware design does not adequately address security concerns. As such, the best solution to reduce the vulnerability and minimize the exploit impact includes a combination of hardware and software.
   2. One potential "short-term workaround until Meltdown is fixed in hardware" is Kernel Page-Table Isolation (KPTI), also known as KAISER. KAISER works by preventing user-space applications from accessing kernel memory directly. This helps enhance the security of the system by minimizing the risk of unauthorized access or exploitation of sensitive kernel data by user-space processes.

.