



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Batch: B1 Roll No.: 16010121045

Experiment No. 1

Title: Cryptanalysis Tools

Objective:

Expected Outcome of Experiment: To implement Cryptanalysis Tools .

CO	Outcome

Books/ Journals/ Websites referred:

<https://resources.infosecinstitute.com/topics/cryptography/cryptanalysis-tools/>



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Abstract:-

Some cryptanalysis tools

Brute force attack

As an old technique, brute force means exhausting very possibility until a match is found. Even in classic cryptography, brute force attack is considered time-consuming.

In modern cryptography, the length of a brute force attack depends exponentially on the length of the key. Since modern cryptography uses very long keys, brute force attack is considered inefficient for all practical purposes.

Chosen plaintext attack

The attacker, in this case, inputs a plaintext and observes the output ciphertext obtained. By examining the plaintext – ciphertext pair, he can easily guess the encryption key. The differential analysis done on RSA algorithm is an example of such attack.

Man in the middle attack

In this type of attack, Eve fools both Alice and Bob. Alice, who wants to communicate with Bob, relays her public key K_a . Eve impersonates Bob and sends her public key K_e . Alice transmits her plaintext P along with K_a & K_e .

Now, Eve has Alice's key as well as the plaintext. She now impersonates Alice and sends her key as Alice's key to Bob. Bob transmits his public key K_b to Eve. To keep Bob from suspecting anything, Eve transmits P along with K_b & K_e to Bob.

Now, Eve has both the public keys of Alice and Bob, as well as the message i.e. the real information she needed.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

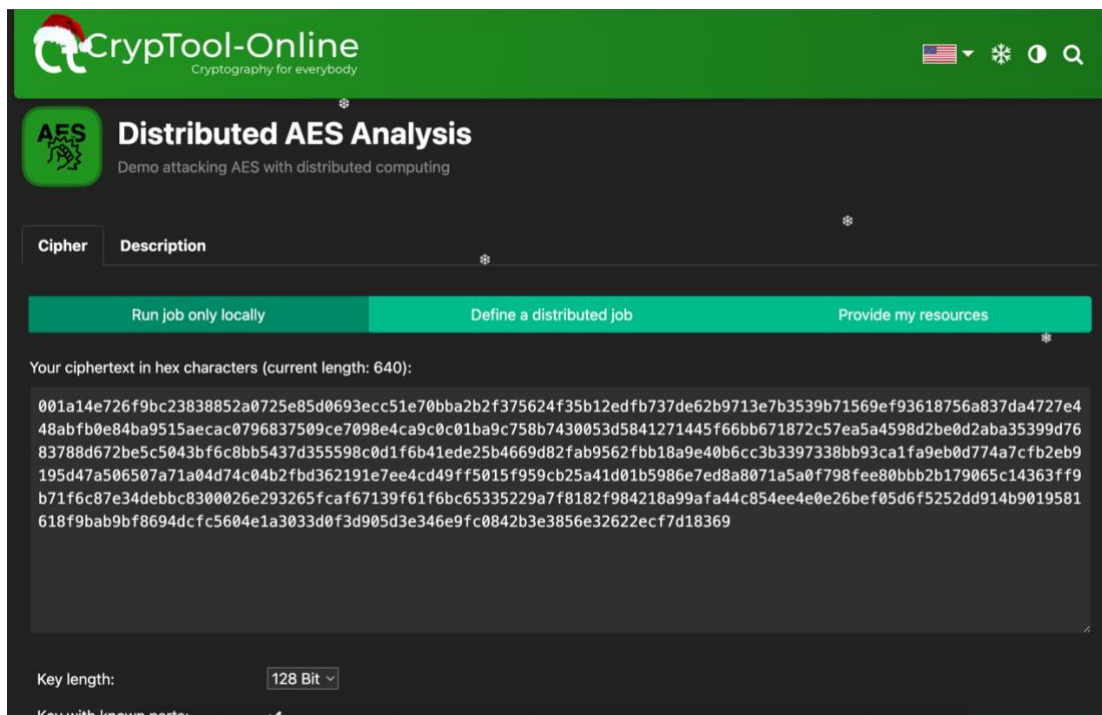
Tools : -

CrypTool

CrypTool was first launched in 1998. It is an e – learning tool explaining cryptanalysis and cryptography. CrypTool aims at making people understand network security threats and working of cryptology. It includes asymmetric ciphers like RSA, elliptic curve cryptography. CrypTool1 (CT1) experiments with different algorithms and runs on Windows. It was developed in C++ language.

CT2, which was launched in 2014, also runs on Windows. It has an improved GUI and more than hundred cryptological functions. It is developed in .NET & C#. JCrypTool (JCT) which followed CT2 is platform independent.

JCT works on Linux, MacOS, and Windows. JCT is both a function – centric as well as a document – centric tool. In 2009, CrypTool – online (CTO) was launched. CTO consists of a huge number of encryption methods and analysis tools. It is a web browser based tool and also targeted at smartphones.





Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Here we can crack AES either alone on your computer, or distributed as a team of many clients who connect their browsers ad-hoc over the internet (assuming, the key is partly known).

The Working

Enter the ciphertext in hexadecimal encoding as full 128-bit blocks (the preset ciphertext consists of 640 hex characters = 2560 bit = 20 full AES blocks).

Select key length: 128, 192, or 256 bits.

Enter the key in hex:

Enter known digits as hex chars (A-F, 0-9).

Mark unknown hex digits with a star (*).

One hex digit correlates with 4 bit. 128 bit correspond to 32 hex digits.

The more * are specified, the longer the analysis takes.

4 stars represent a search space of $16 \text{ bit} = 2^{16} = 65536$ (5 stars = $20 \text{ bit} = 1,048,576$).


Sample: During the testphase beginning 2017, 15 worker threads exhausted a searchspace of 16 bit on a modern laptop in 1:48 min which means a throughput of 605 keys / sec. On a workstation with 31 workers the same search space was exhausted in 0:34 min (throughput 1915 keys / sec).





You can get further information in an overlay windows when clicking on the symbol i (behind key input field).



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Demonstration:

CrypTool-Online
Cryptography for everybody

Cipher

Description

Run job only locally

Define a distributed job

Provide my resources


Your ciphertext in hex characters (current length: 640):





001a14e726f9bc23838852a0725e85d0693ecc51e70bba2b2f375624f35b12edfb737de62b9713e7b3539b71569ef93618756a837da4727e448abfb0e84ba9515aecac0796837509ce7098e4ca9c0c01ba9c758b7430053d5841271445f66bb671872c57ea5a4598d2be0d2aba35399d7683788d672be5c5043bf6c8bb5437d355598c0d1f6b41ede25b4669d82fab9562fbb18a9e40b6cc3b3397338bb93ca1fa9eb0d774a7c fb2eb9195d47a506507a71a04d74c04b2fbd362191e7ee4cd49ff5015f959cb25a41d01b5986e7ed8a8071a5a0f798fee80bb2b179065c14363ff9b71f6c87e34debb8300026e293265fcacf67139f61f6bc65335229a7f8182f984218a99afa44c854ee4e0e26bef05d6f5252dd914b9019581618f9bab9bf8694dcfc5604e1a3033d0f3d905d3e346e9fc0842b3e3856e32622ecf7d18369

Key length: 128 Bit

Key with known parts: ☒

AA ** AA BB ** BB AA BB AA BB AA BB AA BB AA BB

CrypTool-Online
Cryptography for everybody

Key length: 128 Bit

Key with known parts: ☒

AA ** AA BB ** BB AA BB AA BB AA BB AA BB AA BB

Start attack locally

Mode: ECB

Bytes to decrypt per key: 96

Number of workers (local threads): 15

Local job
Computed keys: 65536 / 65536

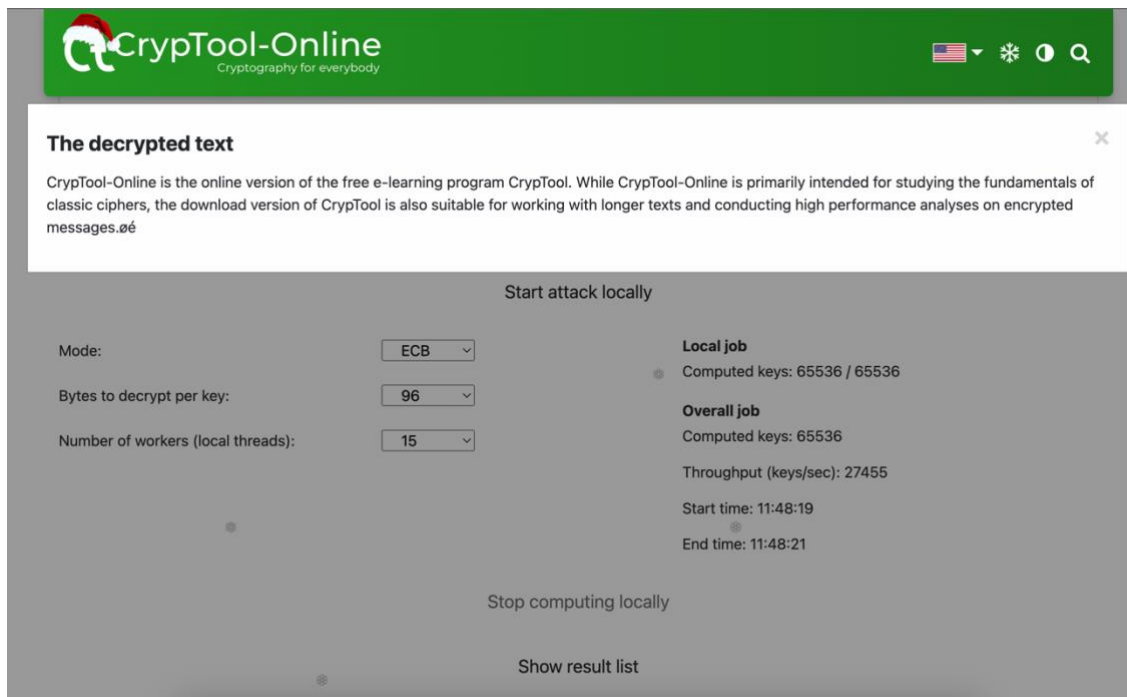
Overall job
Computed keys: 0
Throughput (keys/sec): 0
Start time:
End time:

Stop computing locally

Show result list



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering



EverCrack

An open source GPL software, EverCrack deals chiefly with mono – alphabetic substitution and transposition ciphers. It is a cryptanalysis engine with a multi – language support for English, German, French, Spanish, Italian, Swedish, Dutch and Portuguese. It was initially developed in C language. It is currently concentrating on online web – based applications. Now, the programming is kernel based i.e. deciphering complex ciphers for the kernel.

The overall design goal is to break down complex ciphers systematically into their simplex components for cryptanalysis (by the kernel). The kernel consists of an algebraic design (comparison and reduction) for breaking unilateral, mono – alphabetic ciphers instantaneously. The computational speed is found to be proportional to $O(\log n)$.

An EverCrackGUI looks as shown below.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

EverCrack (GPL) Open Source Cryptanalysis Engine

~Information~

[EverCrack Kernel](#)

[Kernel Source Code](#)

[Essence of Cryptanalysis](#)

[EverCrack TestCloud](#)

EverCrack SiteMap

~Developer~

Cory Michael Boston

[Resume]

Interactive Applications Developer @ Media General

~Online Tools~

[Caesar Cipher Cracker](#)

[Substitution Cipher Cracker](#)

[Matrix Cipher Cracker](#)

[Multilingual to Unilingual Cipher Converter](#)

[Ciphertext Language Identifier](#)

[All Tools](#)

Overview of EverCrack

EverCrack is an Open-Source (GPL) Cryptanalysis Engine. EverCrack performs cryptanalysis on mono-alphabetic substitution and transposition ciphers.

EverCrack currently can crack up to 4000 words in milliseconds - increasing in speed as the size of the cipher text increases making it an O(log n) algorithm in terms of efficiency.

Demo: Let's attempt a brute force attack to crack Caesar Cipher.

How it works: tests each rot result against words in list of that length.

EverCrack Caesar Cipher Cracker

by Dr MindHacker

[\[View PHP Source Code \]](#) [\[How It Works \]](#)

Cipher Text

Uryyb

Crack Cipher

Output:

Cipher Text:

uryyb

Clear Text:

hello

[\[Return to Previous\]](#)



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

dCode.fr

dCode.fr is a set of more than 900 tools to help solve games, puzzles, coded messages, mathematics, etc. dCode is the master of decryption/decoding. Its AI-powered code detector recognizes more than 250 types of ciphers, including the Caesar code, the Vigenère cipher, the Polybius square, as well as dozens of other cryptographic systems. Decrypting messages becomes child's play. dCode offers a huge library of scripts to decode or encode messages with classic cryptography techniques.

The screenshot shows the dCode.fr website. At the top, there's a scroll with the word 'dCODE' on it. Below that, a search bar says 'Find a tool' and 'SEARCH ON dCODE BY KEYWORDS:'. The main content area is divided into sections: 'WORD GAME SOLVERS' (describing dCode as an essential ally for word games), 'TOOLS FOR CRYPTOGRAPHY' (describing dCode as the master of decryption/decoding), and 'TOOLS FOR CODES AND ALPHABETS' (describing dCode as a tool for speaking hundreds of languages). There's also a 'Menu' on the right with links to various tools and a 'Forum/Help' section at the bottom right.

Demo : Vigenère cipher

Cipher Text : ZSXPG KAVDR FLAG UW HODKSH EMFUT



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering



Find a tool

SEARCH ON dCODE BY KEYWORDS:
Type for example 'scrabble'

BROWSE THE FULL LIST OF TOOLS

Vigenère cipher

Tool to decode/encode Vigenere automatically. The Vigenère Cipher is a poly-alphabetic substitution encryption system using a key and a double-entry table.

Vigenère cipher - dCode

Category(s): Poly-Alphabetic Cipher

Share

dCode and more

dCode is free and its tools are a valuable aid in games, math, puzzles, geocaches, and everyday problems to solve!
A suggestion ? a problem ? an idea ? Write to dCode !

VIGENÈRE CIPHER

Cryptography · Poly-Alphabetic Cipher · Vigenère cipher

DECRYPTION OF VIGENERE

MESSAGE ENCRYPTED BY VIGENERE
ZSXPG KAVDR FLAG UW HODKSH EMFUT

SETTINGS

CLEAR MESSAGE LANGUAGE: English

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

DECRYPT AUTOMATICALLY

DECRYPTION METHOD

WITH THE ENCRYPTION KEY/KEYWORD: ADG

WITH KEY LENGTH/SIZE, NUMBER OF LETTERS: 4

WITH JUST A PIECE OF THE KEY: CL?

BY KNOWING A WORD OF THE PLAIN TEXT: HELLO

VIGENERE CRYPTANALYSIS (KASISKI TEST)

DECIPHER

See also: Beaufort Cipher – Caesar Code

ENCRYPTION WITH VIGENERE

CLEAR MESSAGE TO BE ENCRYPTED BY VIGENERE

In the shadows of endpoint/secrets.html, truths hide where the eye doesn't readily see.

ENCRYPTION KEY: CLE

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

MAINTAIN PUNCTUATION

Menu

- Decryption of Vigenere
- Encryption with Vigenere
- What is the Vigenère cipher? (Definition)
- How to encode with Vigenere? (Principle of encryption)
- How to decode by Vigenere? (Principle of decryption)
- How to recognize the Vigenere number?
- How to decipher Vigenere without knowing the key?
- How to find the key with the original text and the corresponding coded text?
- What are the variations of the Vigenere cipher?
- How to choose the encryption key?
- What is vigenere code with current key?
- What is vigenere code with alphabet key?
- What is the Saint-Cyr ruler?
- Why is the Vigenere cipher called that?
- What are the advantages of the Vigenère cipher compared to the Caesar code?
- When was Vigenere invented?

Results

Vigenere 4
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

SOME	HELLO WORLD THIS IS PARGAT SINGH
SOBI	HEWHO WZNLD EDIS TO PACCAT DENG
SOAE	HEXLO WARLD FHIS US PADGAT EINGT
OOM	LELLS WORPD THMS IS TARGET SIRGH
SOBY	HEWRO WZXL D ENIS TY PACMAT DONGS
SOSI	HEFHO WINLD NDIS CO PALCAT MENG
SOAH	HEXIO WAOLD FEIS UP PADDAT EFN
SOBE	HEWLO WZRLD EHS TS PACGAT DING
SOQE	HEHLO WKRLD PHIS ES PANGAT OING
SOMH	HELIO WOOLD TEIS IP PARCAT SFNGH
SOMI	HELHO WONLD TDIS IO PARCAT SENG
SOAI	HEXHO WANLD FDIS UO PADCAT EENG
SOBW	HEWTO WZZLD EPIS TA PACOAT DONG
AOME	ZELLG WORPD THAS IS HARGST SIFGH
OGLH	LMMIS EPOPL UEMA JP TISDEB TFROI
AOMH	ZELIG WOOLD TEAS IP HARDDST SFFGH
SOSE	HEFLO WIRLD NHIS CS PALGAT MING
SOBS	HEWLO WZLD ETIS TE PACSAT DUNG
SOQH	HEHIO WKOLD PEIS EP PANDAT OFNG
SOAS	HEXHO WADLD FTIS UE PADSAT EUNG
SOAY	HEXRO WAXLD FNIS UY PADMAT EONG
SOAC	HEXNO WATLD FJIS UU PADAT EKNG
SOAK	HEXFO WALLD FBIS UM PAAAT ECNG
OOMH	LELLS WOOPD TEMS IP TARDET SFRGH
SOQS	HEHIO WKOLD PTIS EE PANSAT OUNG
SOAJ	HEXGO WAMLD FCIS UN PADBAT EDNG
SOMR	HELYO WOELD TUIS IF PARTAT SVNGH
MOME	NELLU WORRD THOS IS VARGGT SITGH
SOQI	HEHIO WKOLD PDIS EO PANCAT OENG



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Boxentriq

Stuck with a cipher or cryptogram? This tool will help you identify the type of cipher, as well as give you information about possibly useful tools to solve it.

This tool uses AI/Machine Learning technology to recognize over 25 common cipher types and encodings including: Caesar Cipher, Vigenère Cipher (including the autokey variant), Beaufort Cipher (including the autokey variant), Playfair Cipher, Two-Square/Double Playfair Cipher, Columnar Transposition Cipher, Bifid Cipher, Four-Square Cipher, Atbash Cipher, and many more!

The screenshot shows the Boxentriq web application interface. At the top, there is a dark green header with the 'BOXENTRIQ' logo on the left and navigation links 'TOOLS', 'PUZZLE', and 'ABOUT' on the right. Below the header, the main title 'Cipher Identifier and Analyzer' is displayed in white text on a dark green background. A search bar with the placeholder text 'Find Tools...' is located on the right side of the main content area. The main content area has a light gray background and contains the following text: 'Stuck with a cipher or cryptogram? This tool will help you identify the type of cipher, as well as give you information about possibly useful tools to solve it.' followed by a paragraph describing the tool's capabilities. Below this, there is a section titled 'Enter Ciphertext here' with a large text input field containing the sample ciphertext 'Svool dliow gsrh rh kzitzg hrmts sviv!'. Under the input field, there are four green buttons: 'Analyze Text', 'Copy', 'Paste', and 'Text Options...'. At the bottom of the section, a note states: 'Note: To get accurate results, your ciphertext should be at least 25 characters long.'

Conclusion:- Learnt to use and implement various cryptographic tools.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Postlab questions:

1.1 Write the points of difference between mono-alphabetic cipher and polyalphabetic cipher.

SR.NO	Monoalphabetic Cipher	Polyalphabetic Cipher
1	Monoalphabetic cipher is one where each symbol in plain text is mapped to a fixed symbol in cipher text.	Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
2	The relationship between a character in the plain text and the characters in the cipher text is one-to-one.	The relationship between a character in the plain text and the characters in the cipher text is one-to-many.
3	Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.	Each alphabetic character of plain text can be mapped onto 'm' alphabetic characters of a cipher text.
4	A stream cipher is a monoalphabetic cipher if the value of key does not depend on the position of the plain text character in the plain text stream.	A stream cipher is a polyalphabetic cipher if the value of key does depend on the position of the plain text character in the plain text stream.
5	It includes additive, multiplicative, affine and monoalphabetic substitution cipher.	It includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor, and Enigma cipher.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

1.2 Explain the working of a rail-fence cipher with the help of an example.

Given a plain-text message and a numeric key, cipher/de-cipher the given text using Rail Fence algorithm.

The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.

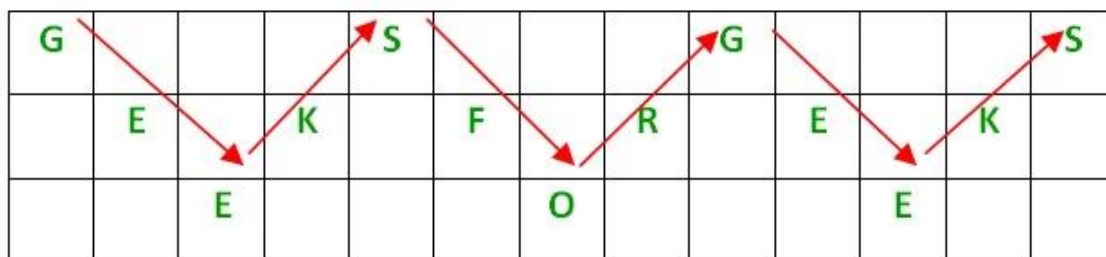
Examples:

Encryption

In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

- In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence.
- When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus the alphabets of the message are written in a zig-zag manner.
- After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

For example, if the message is “GeeksforGeeks” and the number of rails = 3 then cipher is prepared as:



© copyright geeksforgeeks.org

∴ Its encryption will be done row wise i.e. GSGSEKFREKEOE

Decryption

As we've seen earlier, the number of columns in rail fence cipher remains equal to the length of plain-text message. And the key corresponds to the number of rails.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

- Hence, rail matrix can be constructed accordingly. Once we've got the matrix we can figure-out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively).
- Then, we fill the cipher-text row wise. After filling it, we traverse the matrix in zig-zag manner to obtain the original text.

Implementation:

Let cipher-text = "GsGsekre eoe" , and Key = 3

- Number of columns in matrix = $\text{len}(\text{cipher-text}) = 13$
- Number of rows = key = 3

1.3 Discuss any three applications of cryptography.

- Cryptography is widely used to secure communication over the internet. Protocols like HTTPS use cryptographic techniques to encrypt data exchanged between web browsers and servers, ensuring privacy and integrity.

2. Digital Signatures:

- Cryptography is employed in creating digital signatures, which authenticate the origin and integrity of digital messages or documents. Digital signatures are crucial in electronic transactions and document verification.

3. Data Encryption:

- Cryptography is extensively used to encrypt sensitive data stored on various devices or transmitted over networks. This protects information from unauthorized access and ensures confidentiality. Technologies like BitLocker and FileVault employ encryption to secure data on storage devices.