**CRYPTOGRAPHY TERMINOLOGY**

**CRYPTOGRAPHY**

*The science of transforming information so that it is secure while being transmitted or stored.*

*This done by scrambling the data so that it cannot be viewed by unauthorized users.*

**STEGANOGRAPHY**

*Steganography attempts to hide the existence of the data.*

**ENCRYPTION**

*Changing the original text to a secret message using cryptography is known as encryption.*

**DECRYPTION**

*Change the secret message back to its original form. The reverse process of encryption.*

**ALGORITHM**

*The process of encrypting and decrypting information is based on a mathematical procedure called an algorithm*

**KEY**

*A value that is used by an algorithm to encrypt or decrypt a message.*

**PLAINTEXT**

*This is the original unencrypted information*

**CIPHER**

*A cipher is an encryption or decryption algorithm tool that is used to create encrypted or decrypted text.*

**CIPHERTEXT**

*Data that has been encrypted by an encryption algorithm (a cipher) is called* ***ciphertext****.*

**HOW CRYPTOGRAPHY PROVIDES SECURITY ?**

|  |  |
| --- | --- |
| **Protection** | **Description** |
| Confidentiality | Allow only authorized users to access the information |
| Authentication | Verify who the sender was and trust the sender is who the claim to be. |
| Integrity | Trust the information has not been altered |

**EXERCISE 1**

**Encrypt these messages using a Caesar cipher**:

1. ABBI IS INCREDIBLY AWESOME.

2. I LOVE COLLEGE ALGEBRA.

3. WE ARE THE ANOKA FAMILY.

4. WINTER IS SUPER COLD.

5. SENIORS ROCK MY SOCKS.

**EXERCISE 2**

**Decipher these messages using a Caesar cipher:**

1. FDFLH FDUUROO HQMRBV PDWK

2. VXEZDB VDQGZLFKHV DUH WDVWB

3. PLQQHVRWD JRSKHUV

4. FKRFRODWH PDNHV WKH ZRUOG JR URXQG

5. IXCCB VZHDWHUV NHHS BRX

**EXERCISE 3**   
Each of the following messages has been encrypted using a simple substitution cipher. Decrypt them.

JNRZR BNIGI BJRGZ IZLQR OTDNJ GRIHT USDKR ZZWLG OIBTM NRGJN  
IJTZJ LZISJ NRSBL QVRSI ORIQT QDEKJ JNRQW GLOFN IJTZX QLFQL  
WBIMJ ITQXT HHTBL KUHQL JZKMM LZRNT OBIMI EURLW BLQZJ GKBJT  
QDIQS LWJNR OLGRI EZJGK ZRBGS MJLDG IMNZT OIHRK MOSOT QHIJL  
QBRJN IJJNT ZFIZL WIZTO MURZM RBTRZ ZKBNN LFRVR GIZFL KUHIM  
MRIGJ LJNRB GKHRT QJRUU RBJLW JNRZI TULGI EZLUK JRUST QZLUK  
EURFT JNLKJ JNRXR

**EXERCISE 1 - SOLUTION :**

1. DEEL LV LQFUHGLEOB DZHVRPH
2. L ORYH FROOHJH DOJHEUD
3. ZH DUH WKH DQRND IDPLOB
4. ZLQWHU LV VXSHU FROG
5. VHQLRUV URFN PB VRFNV

**EXERCISE 2 - SOLUTION**

* CACIE CARROLL ENJOYS MATH
* SUBWAY SANDWICHES ARE TASTY
* MINNESOTA GOPHERS
* CHOCOLATE MAKES THE WORLD GO ROUND
* FUZZY SWEATERS KEEP YOU WARM