Long Island STEM Hub

Bringing Industry and Education Together

NEW YORK INSTITUTE OF TECHNOLOGY

Cybersecurity Exercise 1 | Encrypt & Decrypt a Secret Message

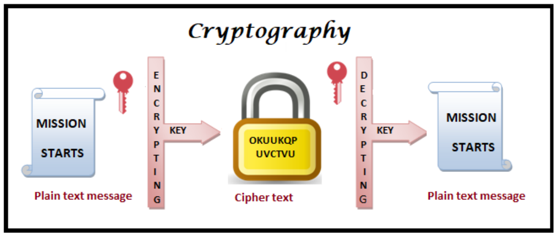
CYBERSECURITY | 6TH – 12TH GRADES

Cybersecurity

Cybersecurity is one of the fastest growing technology sectors today. With 11 billion currently connected Internet devices and a forecast of 20 billion connected devices by the year 2022, there has never been more access points and vulnerabilities to our sensitive and valuable data than there is today. Because of this, there is an ongoing cybersecurity workforce gap making it increasingly difficult for organizations to find cybersecurity analysts, application security experts, and security leaders at the executive level. One of the most effective ways to protect data is to encrypt it. This exercise is designed to introduce students to various methods of encryption but also to introduce them to the bold new career frontier known as Cybersecurity.

Cryptography is technique of securing information and communications using codes so that only the person for whom the information is intended can understand it and process it thus preventing unauthorized access to information. In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions.

In cryptography, **encryption** is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Only authorized parties can decipher a ciphertext back to plaintext and access the original information.



"Codes are a puzzle. A game, just like any other game." - Alan Turing

Historical & Modern Encryption Methods

Here are a few popular historical encryption methods that have been used through the ages to protect secret messages. Since encryption algorithms and methods get cracked and compromised all the time, new ones always have to be created that are more complex and difficult to break. Below are a combination of some simple early ciphers along with today's modern encryption methods in use today. After you review them, work through the exercise and try and encrypt and decrypt your own secret messages just like a computer!

Historical Methods of Encryption

Caesar Shift Cipher

ROT 13 Cipher

Substitution Cipher

Modern Day Encryption Methods

Data Encryption Standards (DES)

Advanced Encryption Standards (AES)

Secure Hash Algorithm (SHA-2)

The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is named after Julius Caesar, who apparently used it to communicate with his generals.

The ROT13 cipher is a substitution cipher with a specific key where the letters of the alphabet are offset 13 places. I.e. all 'A's are replaced with 'N's, all 'B's are replaced with 'O's, and so on. It can also be thought of as a Caesar cipher with a shift of 13.

In cryptography, a substitution cipher is a method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth.

Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a private key. Unlike symmetric key algorithms that rely on one key to both encrypt and decrypt, each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt.

SHA is an abbreviation for Secure Hash Algorithm, which is a group of cryptographic hash functions developed by the US National Security Agency (NSA).
SHA hash functions are used by Certificate Authorities when signing Certificate Revocation Lists and Digital Certificates. A Secure Hash Algorithm is meant to generate unique hash values from files.

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection.

Encryption Hands-On Exercises

1. Decrypt the following message:

ORQJ LVODQG VWHP KXE

Hint: In **Rome**, there are at least **3** famous structures

2. Decrypt the following message:

ARJ LBEX VAFGVGHGR BS GRPUABYBTL

Hint: How **many** original U.S. colonies were there again?

3. Decrypt the following message:

021700031104 1405 0021080019081413

Hint: A **substitute** teacher once told me that the letter A was equal to **zero**.

Directions:

Step 1. Detrmine from the hints which type of enryption was used to encode the messages.

Step 2. Use a tool like http://rumkin.com/tools/cipher/ to help you try and decode the message.

Step 3. Record your answers on the next page.

Record Your Answers Below

ORQJ LVODQG VWHP KXE

Decrypted Message:

____

ARJ LBEX VAFGVGHGR BS GRPUABYBTL

Decrypted Message:

____

021700031104 1405 0021080019081413

Decrypted Message:

____

"Cryptography is typically bypassed, not penetrated" - Adi Shamir

Website:
www.nyit.edu
www.listemhub.org

Contact:
Dr. Michael Nizich
516-686-1360

Email:
mnizich@nyit.edu

NEW YORK INSTITUTE
OF TECHNOLOGY

College of Engineering
& Computing Sciences