TUTORIAL

CRYPTOGRAPH

Y

Purpose

- ✓ Understand the importance of checksum value to check file integrity
- ✓ Understand principles of encryption (XOR operations, binary conversion)
- ✓ Able to send encrypted message & decrypt the encrypted message

Class Activities

1. ACSII to hexadecimal and binary

- Estimated duration: 15 mins

Students download the file (ASCII-to-hex-bi) from FIT portal and study it.

Discussion 1: Students are expected to answer the following questions after reading (20 mins)

- Convert plaintext 'Hello world' into binary and hexadecimal.

- How many bits are there?

- Using key "itsimplekey" and XOR operator to create a cipher. *Hints:* Convert both plaintext and key into binary to make XOR operation.

- Covert the result to Hexadecimal.

- Check it out at: *http://www.rapidtables.com/convert/number/ascii-to-binary.htm* and http://xor.pw/

2. Hashing algorithm

- Estimated duration: 10 mins

CertUtil is a pre-installed Windows utility that can be used to generate hash checksums:

```
certUtil -hashfile pathToFileToCheck
[HashAlgorithm]
```

HashAlgorithm choices: MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512

Download the Unikey software from FIT

portal. Save it to Desktop, rename it as

unikey.exe

Open CMD, change working directory to Desktop

Use *certutil* command to see hash value of the file.

```
C:\Users\ADMIN>cd Desktop

C:\Users\ADMIN\Desktop>certutil -hashfile unikey.exe
SHA1 hash of unikey.exe:
c698a001358459252c089bfe55f591f80d141e17
CertUtil: -hashfile command completed successfully.
```

Go to this website: http://unikey.vn/vietnam/#nav4 to view checksum of original file. Tell me the file downloaded from FIT portal is modified or not, compared to the original file from its official site.

3. Practice with Instant Crypt

Instant Crypt is a program that allows you to send encrypted message using the model of asymmetric encryption. In this practice, you need to generate your own key pairs first and then exchange your public key with

a. Create their own keys

- Estimated Duration: 10 mins

Each student copies/downloads InstantCrypt and makes installation. After installation, students follow the demo video to generate their key pair.

Demo is available at:
http://www.instantcrypt.com/onlinehelp/demos/KeyCreate.htm

b. Exchange public keys

- Estimated Duration: 15 mins

Export your public keys: *Key Management* > *Export own public keys* > *Choose folders to save it.* Send your own public key to your partner via email or file sharing. Your partner does the same. Both of you create your own public keys and send to each other.

When receiving your friend's public key, import it: *Key Management* > *Import Key*

c. Encrypting messages

- Estimated Duration: 10 mins

Work in the same group. You are required to create an encrypted message and email it to your partner.

Demo is available at:

http://www.instantcrypt.com/onlinehelp/demos/FirstEncryption.htm

Discussion 2: In this activity, students are expected to answer the following questions:

What is the purpose of exchanging their keys?

d. Decrypting messages

- Estimated Duration: 10 mins

Work in the same group. Open the encrypted messages sent from your partner and try to decrypt the message.

Demo is available at:

http://www.instantcrypt.com/onlinehelp/demos/FirstDecryption.htm

References

http://www.instantcrypt.com/InstantCrypt_Support.php