Nature Sunday Academy Lesson Plan – 2013-14

Title – Computer Security

Description:

The objective of the lesson plan aims to help students to understand the general goals of security, the essential concerns in achieving the general goals of security, a few cryptographic methods, and the weakness of a cryptographic method. This lesson plan includes three hands-on activities.

The first activity allows students to practice 3 examples of symmetric-key cryptosystem. In each of these examples, students will first learn the basic idea of the encryption/decryption method. Then, students will work on concrete samples to encrypt/decrypt a short text. Meanwhile, students will be exposed to the weakness of a cryptosystem.

The second activity allows students to learn the way that an asymmetric-key cryptosystem works. Students will play a hands-on game to see the difference in difficulty of decrypting a cipher text when the private key is known and unknown.

The third activity allows students to learn the simple methods of detecting the unwanted changes made on the text. Students will practice on 1-dimensional and 2-dimensional parity checking.

The fourth activity allows students to see how the digital signature systems work.

Cultural Connection:

Session Organization:

11:00 -- 11:15 AM -- Cultural Connection

11:15 -- 11:45 AM -- Introduction

11:45 -- 12:00 PM -- Activity 1: Hands-on Practice on Symmetric-Key Ciphers.

12:00 -- 12:30 PM -- Lunch

12:30 -- 1:00 PM -- continue on with Activity 1

1:00 -- 2:00 PM -- Activity 2: Hands-on Practice on Asymmetric-Key Ciphers.

2:00 -- 2.45 PM -- Activity 3: Zero-Knowledge Proof

2:45 -- 3:00 PM -- Wrap-up and Evaluation

Vocabulary – Definitions:

Confidentiality: hiding the true meaning of information.

Integrity: information without unauthorized changes.

Availability: information can be accessible at all times.

Symmetric-key Ciphers: the same key is shared between a pair of sender and receiver.

Asymmetric-key Cryptography: different keys are used by a pair of sender and receiver.

Digital Signatures: the procedure of digitally signing a document based on asymmetric-key cryptography.

Activity 1:

Summary

Students will look into a few examples of symmetric-key ciphers to see how they work. Three examples will be introduced: mono-alphabetic substitution cipher, poly-alphabetic substitution cipher, and transposition cipher.

Requirements

Students form groups of two persons. Each group will work on examples printed on a sheet of paper.

Example 1 (mono-alphabetic substitution cipher)

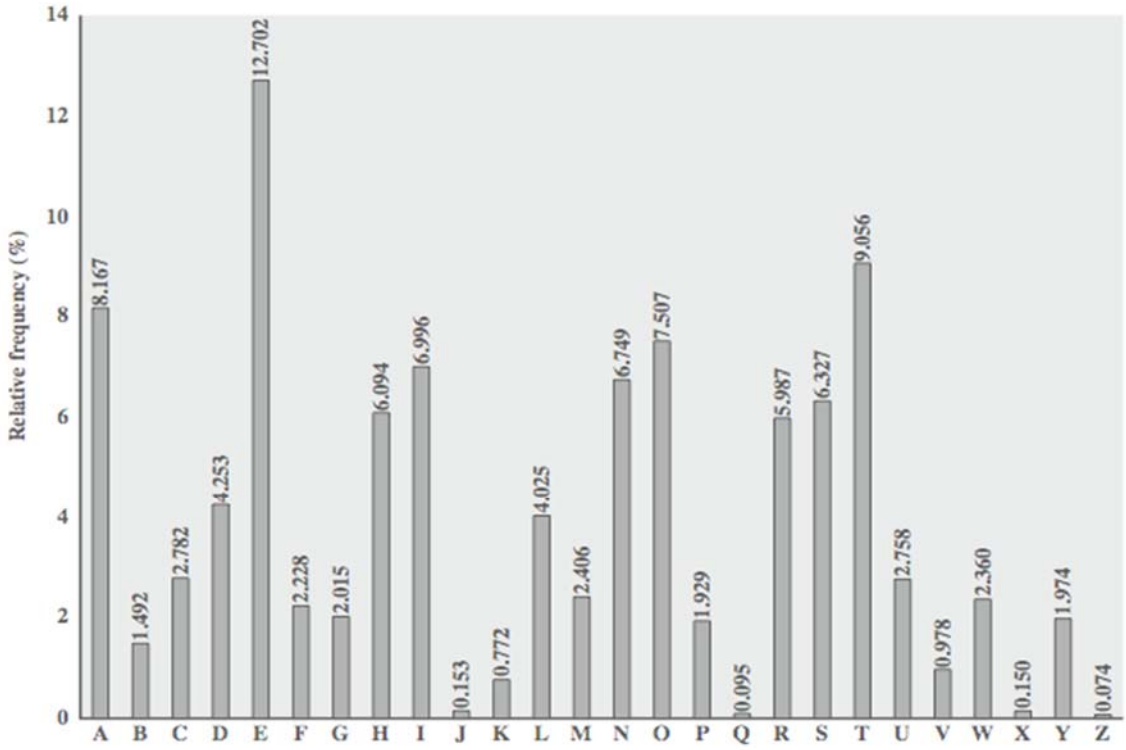
1. The famous example of the mono-alphabetic substitution cipher is Caesar cipher.
2. It replaces each letter by the 3rd letter on the right. The key is 3.
3. The transformation is defined as

   Plaintext a b c d e f g h i j k l m n o p q r s t u v w x y z

   Ciphertext D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

4. The security ability of the mono-alphabetic substitution cipher is very limited because that the key can be found by trying all possible shifts until a meaningful text is exposed.
5. Another systematic way of cracking the mono-alphabetic substitution cipher is to use the features in English language.

a. Human languages are **redundant**, and characters are not equally commonly used.
b. In English, E is by far the most common letter, followed by T,R,N,I,O,A,S.
c. Other letters like Z,J,K,Q,X are fairly rare.



d. Mono-alphabetic substitution ciphers do not change the relative letter frequencies.
e. Attackers can simply calculate the letter frequencies for cipher text and compare the counts against known values.
f. To solve the ties, tables of common double/triple letters help a lot.
g. Example:
    - given cipher text:

      UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETS
      XAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHS
      XEPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

    - count relative letter frequencies.

      P Z U S O M H D E X V W F T Q Y G A B Y I J

      16 14 10 10 9 8 7 6 6 5 5 4 4 3 3 2 2 2 2 2 1 1

    - guess *P* and *Z* are *e* and *t*, respectively.
    - guess *ZW* is *th* and hence *ZWP* is *the*.

- proceed with trial and error, and finally get:

it was disclosed yesterday that several informal but
direct contacts have been made with political representatives
of the viet cong in moscow

Example 2 (poly-alphabetic substitution cipher)

1. The simplest example of the polyalphabetic substitution ciphers is the **Vigenère cipher**.
2. Poly-alphabetic substitution ciphers improve the security of mono-alphabetic substitution ciphers by using multiple letters.
3. Poly-alphabetic substitution ciphers make cryptanalysis harder with the flatter frequency distribution.
4. A key is multiple letters long $K = k_1\ k_2\ ...\ k_d$
    a. The i^{th} letter specifies i^{th} alphabet to use.
    b. Use each alphabet in turn.
    c. Repeat from start after d letters in message.
    d. Decryption simply works in reverse.
5. An Example of Vigenère Cipher
    a. The keyword: *deceptive*
    b. Original message: **we are discovered, save yourself.**
    c. plaintext: wearediscoveredsaveyourself
    d. key: deceptivedeceptivedeceptive
    e. shifts: d e c e p t i v e

       3 4 2 4 15 19 8 21 4

       session 1|session 2|session 3

       key: deceptive|deceptive|deceptive

       plaintext: wearedisc|overedsav|eyourself

       ciphertext: ZICVTWQNG|RZGVTWAVZ|HCQYGLMGJ

    f. Relative frequency (flatter)

       G V Z C T W Q A M I J L N R Y

       4 3 3 2 2 2 2 1 1 1 1 1 1 1 1
6. Security of Vigenère Cipher
    a. The letter frequencies are obscured because that one plaintext letter may correspond to multiple ciphertext.

b. But, the letter frequencies are not totally lost.

Example 3 (transposition cipher)

1. The transposition cipher is to first divide the plaintext into groups of predetermined size, called blocks.
2. Then, a key is used to permute the characters in each block separately. The encryption key is the size of the blocks.
3. The cipher text has the same frequency distribution as the original text.
4. An example of the transposition cipher:
    a. Plaintext: ‘WE ARE DISCOVERED. FLEE AT ONCE’
    b. The key is 6.
    c. First, removing the punctuations and write the text in a row:

        WEAREDISCOVEREDFLEEATONCE

    d. Then, organizing the plaintext into a block for a block size of 6:

        WEARED
        ISCOVE
        REDFLE
        EATONC
        EQKJEU

    e. Next, reading the text column-wise and putting the text into a row to form the cipher:
    WIREE ESEAQ ACDTK ROFOJ EVLNE DEECU

    f. Restoring the plaintext from the cipher text requires to know the block size. The block size is the secret which is only known to Alice and Bob.
5. An exercise:
    a. Cipher text:

        WIESHNMSEGEONWMUDABRRTECIERENRIZKRTZ

    b. What is the plain text?
    c. Hint: You have to guess the size of the block.
    d. Time limit: 1 minute.

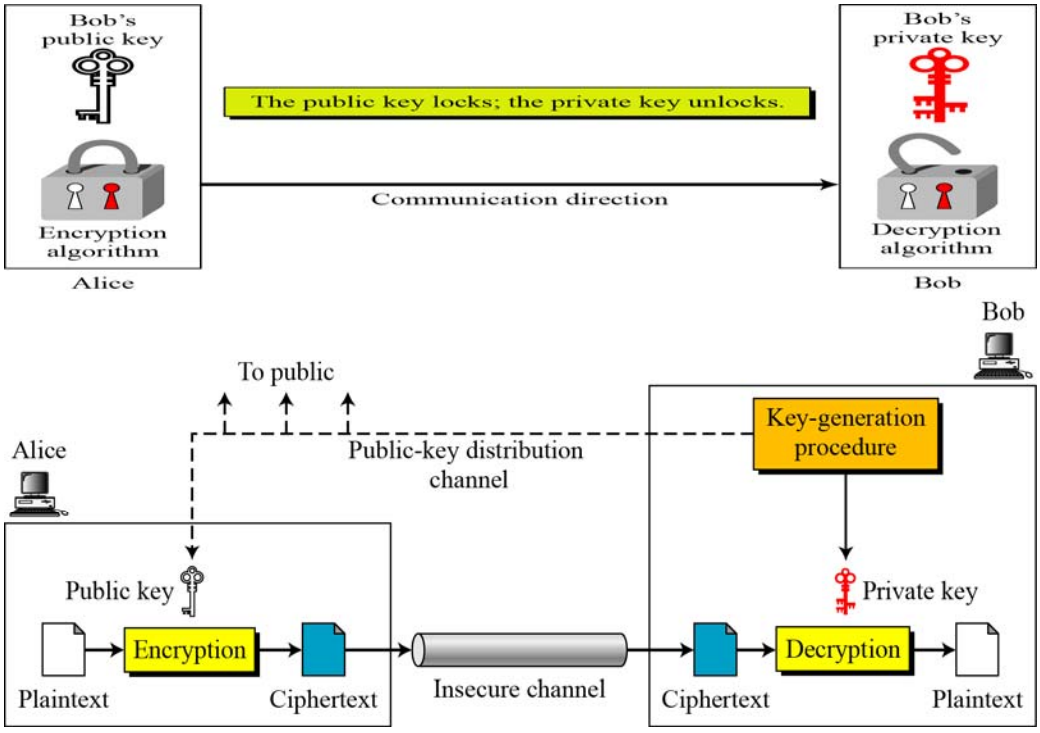
Activity 2

Summary

- Symmetric-key cryptography is based on sharing secrecy between Alice and Bob. The shared key has to be updated periodically. It is difficult to send the new key to Alice and Bob. There is a need that the secrecy is not sent. The solution is

the asymmetric-key cryptography that is based on personal secrecy. Asymmetric-key cryptography uses two separate keys: one private key and one public key.

- The private key is never sent out from the key owner.
- The public key is supposed to be known by everyone in the world.
- Plaintext and cipher text are treated as integers in asymmetric-key cryptography.
- The main idea behind asymmetric-key cryptography is the concept of the trapdoor one-way function.



Example 1 (The One-Way Function)

1. For two large prime numbers *p* and *q.*
2. $n = p \times q$ is a one-way function.
3. Given *p* and *q*, it is always easy to calculate *n*;
4. Given *n*, it is very difficult to compute *p* and *q* when *p* and *q* are large.
5. When given *n* and one of the factors, it becomes easy to calculate the other factor.
6. An easy calculation: When p=11, q=19, we can quickly calculate $n=p \times q = 11 \times 19 = 209$.
7. A difficult calculation: Given that $n=p \times q = 221$, what are the values of p and q?

Example 2 (The Trap-Door One-Way Function)

1. A difficult calculation:
    a. Given a sequence [295, 592, 301, 14, 28, 353, 120, 236] and a value *1129.*
    b. It is known that the value *1129* is a sum of a portion of the sequence.
    c. Can you quickly figure out the items in the sequence, which are used to form the value of *1129?*
2. An easy calculation:
    a. Given a new sequence [2, 7, 11, 21, 42, 89, 180, 354] and a value 372.
    b. It is known that the value 372 is a sum of a portion of the sequence.
    c. Can you quickly figure out the items in the sequence, which are used to form the value of 372*?*
    d. The sequence [2, 7, 11, 21, 42, 89, 180, 354] is super-increasing.
    e. The decomposition of 372 is very easy.

354	**372 - 1*354 = 18**	**1**
180	**18 - 0*180 = 18**	**0**
89	**18 - 0*89 = 18**	**0**
42	**18 - 0*42 = 18**	**0**
21	**18 - 0*21 = 18**	**0**
11	**18 - 1*11 = 7**	**1**
7	**7 - 1*7 = 0**	**1**
2	**0 - 0*2 = 0**	**0**

3. The difficult calculation is generated from the easy calculation.
    a. The sequence [2, 7, 11, 21, 42, 89, 180, 354] and an integer 588 are used the private key.
    b. The key owner generate the public and private keys from the super-increasing sequence [2, 7, 11, 21, 42, 89, 180, 354]:
        i. First, calculate the sum of the sequence [2, 7, 11, 21, 42, 89, 180, 354]. The sum is 706.
        ii. Choose an integer *n* that is larger than 706. We choose *n=881*.
        iii. Choose an integer *r* that is mutually prime with 811. We choose *r=588*.
        iv. Calculate the inverse of *r* as $r^{-1}=442$ with $r \times r^{-1}=1 \bmod 881$.
        v. The sequence [2, 7, 11, 21, 42, 89, 180, 354], n=881, and *r=588* are used as the private key.

vi. The public key is calculated as [295, 592, 301, 14, 28, 353, 120, 236] with

(2 × 588) mod 881 = 295
(7 ×588) mod 881 = 592
(11 × 588) mod 881 = 301
(21 × 588) mod 881 = 14
(42 × 588) mod 881 = 28
(89 × 588) mod 881 = 353
(180 × 588) mod 881 = 120
(354 × 588) mod 881 = 236

4. Secret Communications using the asymmetric key encryption system.

Requirements

Students form groups of two persons: an encoder and a decoder. Each group will work on examples printed on a sheet of paper.

Procedure

1. Each encoder is assigned with an 8-bits binary number representing a character. For example, the binary bits *01100001* represent a character 'a'.
2. Each decoder is assigned with a pair of private and public keys.
3. The decoder in a group informs the encoder about his public key.
4. The encoder tries to send the assigned 8-bits binary number in an encrypted form to the decoder in the same group.
5. After generating the cipher text of a plaintext, the encoder sends the cipher text to all the decoders in the classroom.
    a. For example, using the public key [295, 592, 301, 14, 28, 353, 120, 236], character 'a' is encoded into a cipher text C=*1129* which is computed by

    $1129=0\times295 + 1\times592 + 1\times301 + 0\times14 + 0\times28 + 0\times353 + 0\times120 + 1\times236$

    b. Pay close attention to the alignment of the public key and the binary bits.
6. Each decoder tries to figure out the plaintext of the cipher text.
    a. An example of decoding C=*1129*
        i. Using the private key of [2, 7, 11, 21, 42, 89, 180, 354], n=881, and *r=588*
        ii. First, convert C=*1129 into C' by*

        $C' = C\times r^{-1} \bmod n = 1129\times442 \bmod 881 = 372.$

        iii. Next, restoring the plain text by the following decomposition:

354	***372 - 1×354 = 18***	***1***
180	***18 - 0×180 = 18***	***0***
89	***18 - 0×89 = 18***	***0***
42	***18 - 0×42 = 18***	***0***
21	***18 - 0×21 = 18***	***0***
11	***18 - 1×11 = 7***	***1***
7	***7 - 1×7 = 0***	***1***
2	***0 - 0×2 = 0***	***0***

iv. The binary bits are *01100001* which represents 'a'.

Questions

1. Can a decoder restore the plaintext from every piece of the cipher text?
2. How does a decoder know a decryption is correct?

Activity 3

Summary

In many situations, there is a need to convince someone that you have the solution to a problem, without revealing any detail of your solution to others. The method of zero-knowledge proof is a viable approach to deal with the problem of proving the truthfulness of a solution without revealing any detail. The proof consists of a prover and a verifier. The prover interacts with the verifier to prove the truthfulness of the solution. The proof is to design a conversation between the verifier and the prover, without making verifier to know anything about the secret of the prover.

Requirements

Students act as the verifiers, and the instructor acts as the prover. The prover shows the correctness of the solution to a Sudoku puzzle without disclosing any detail of the solution.

Procedure

1. A Sudoku puzzle is first described to students.
2. The requirement of a correct solution to a Sudoku puzzle is described.
3. The Sudoku puzzle is demonstrated using a cardboard.
4. The prover claims to have a solution to a Sudoku puzzle.

5. The verifiers examine the correctness of the solution.
6. Through the process of examining the solution, the verifiers know nothing about the detail of the solution.