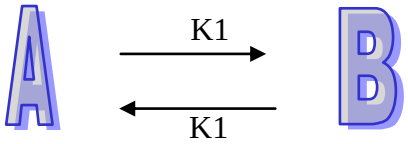
Subject :	SEHH2238 : Computer Networking
Lab/Tutorial :	Session 10 : Network Security (Solution)

A. Symmetric Cryptography

1. In symmetric-key cryptography, how many secret keys are needed, if every person in a group of 10 people needs to communicate with
   a) Every other person in another group of 10 people
   b) Every other person in the same group

   a) Every person has to communicate with 10 people, he has to have 10 keys.
   Total no. of keys = 10 x 10 =100
   b) Similar to mesh network.
   For the first people, he needs 9 keys to communicate with the others.
   For the second one, he needs 8 new keys as the key for communicating with first one was already counted.
   Total no. of keys = 9 + 8+ 7…+ 1 = 45.
   OR = $_{10}C_{2}$ = 10!/(8! X 2!) = 45

   The above assumes the two-way communication can use the same key.



2. Encrypt the message "THIS IS AN EXERCISE" using a shift cipher with a key of 20. Ignore the space between words

Idx: 0 5 10 13 15 20 25
Char: 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
"T": The original index 19. The new index (19 +20) mod 26 = 39 mod 26 =13
The encrypted char "N"
"H": New index: (7 + 20) mod 26 = 1. The encrypted char "B"
"I": New index: (8 + 20) mod 26 = 2. The encrypted char "C"
..
The encrypted message: "NBCM CM UH YRYLWCMY"

3. Encrypt "INTERNET" using a transposition cipher with the following key: 4 3 1 5 2

```
Post:       1 2 3 4 5
Char:       I N T E R
            N E T Z Z   ( Z is a dummy character)

New post:   3 5 2 1 4
Char:       T R N I E
            T Z E N Z
```

The encrypted message: T R N I E T Z E N Z

B. Security

What are the DO's and DON'Ts for handling accounts & passwords?

<<You can search for the Internet>>

http://www.infosec.gov.hk/english/yourself/account.html

DO'S

- Use a password with a mix of at least six mixed-case alphabetic characters, numerals and special characters.
- Use a password that is difficult to guess but easy for you to remember, so you do not have to write it down.
- Use a password that you can type quickly, without having to look at the keyboard, thereby preventing passers-by seeing what you are typing.
- Change your password frequently, at least once every 90 days.
- Change the default or initial password the first time you login.
- Change your password immediately if you believe that it has been compromised. Once done, notify the system/security administrator for follow up action.
- Log off when finished using terminals or PCs in public areas, such as a library or cafe.

DON'TS

- Don't use your own name as a login name in any form (as-is, reversed, capitalised, doubled, etc).
- Don't use the name of your spouse or child in any form.
- Don't use other information that might be easily obtained about you. This includes ID card numbers, license numbers, telephone numbers, birth dates, the name of the street you live on, and so on.
- Don't use a password that contains all digits, or all the same letters.
- Don't use consecutive letters or numbers like "abcdefgh" or "23456789".
- Don't use adjacent keys on the keyboard like "qwertyui".
- Don't use a word that can be found in an English or foreign language dictionary.
- Don't use a word in reverse that can be found in an English or foreign language dictionary.
- Don't use a well-known abbreviation e.g. HKSAR, HKMA, MTR.
- Don't reuse recently used passwords.
- Don't use the same password for everything; have one password for non-

critical activities and another for sensitive or critical activities.

- Don't write down your password, particularly anywhere near your computer or file it in a box file with the word 'password' written on it.
- Don't tell or give out your passwords to other people, even for a very good reason.
- Don't display your password on the monitor.
- Don't send your password unencrypted, especially via email.
- Avoid using the "remember your password" feature associated with some websites, and disable this feature in your browser software.
- Don't store your password on any media unless it is protected from unauthorised access (e.g. encrypted with an approved encryption method).

B. Asymmetric Cryptography

4. In RSA, given two prime numbers p=19 and q=23, find n and ϕ. Choose e = 5 and try to find d, such that e and d meet the criteria.

n = p x q = 19 x 23 = 437
Φ = (p-1) x (q-1) = 18 x 22 = 396
Check e x d mod Φ = 1,

Now 5 x d mod 396 = 1
- ⇨ 5 x d = m x 396 + 1 where d and m are integers
- ⇨ d =(m x 396 + 1) /5

Try m =1, 2, 3, … until d is an integer.
If there are multiple values of d fulfill the requirement, we could just choose one of them.

To prove d=317 is valid key (when m = 4),

5 x 317 mod 396 = 1585 mod 396 =1
So, e=5 and d=317 are valid.

5. What is the danger in choosing 2 as the public key e in RSA?

Knowing that n is very large and $C = P^e \bmod n$.
If e is small and P is not large, $C = P^e$.
E.g. P =16, e = 2, n =23423, $C = 16^2 \bmod 23423 = 256$
P can be easily found by taking root on C, as $P = C^{1/2}$.
It will be easy to guess P.