## Activities - cryptography lecture 02

**Activity 01**

- Convert “AYUBOWAN

  DBXERZDQ

- Convert “TREATY IMPOSSIBLE” using the substitution key K=5

  YWJFYD NRUTXXNGQJ

**Activity 02**

- Compare Block Vs Stream Cipher.

| | Block | Stream |
|---|---|---|
| How it works | A block cipher encrypts data in blocks using a deterministic algorithm and a symmetric key. Block ciphers, on the other hand, encrypt 128 bit blocks with a key of predetermined length: 128, 192, or 256 bits. ... A 128-bit block cipher brings 128 bits of plaintext and encrypts it into 128 bits of cipher text. | Stream cipher encrypts data one bit at a time instead of in blocks. But a key part of this process is generating a stream of pseudorandom bits based on an encryption key and a seed. Together, they create a keystream that gets XORed with your plaintext input, which encrypts it and results in your cipher text output. |
| Advantages | • High diffusion: information from one plaintext symbol is diffused into several cipher text symbols.<br>• Immunity to tampering: difficult to insert symbols without detection. | • Speed of transformation: algorithms are linear in time and constant in space.<br>• Low error propagation: an error in encrypting one symbol likely will not affect subsequent symbols. |

| | | |
|---|---|---|
| Disadvantages | • Slowness of encryption: an entire block must be accumulated before encryption / decryption can begin.<br>• Error propagation: An error in one symbol may corrupt the entire block. | • Low diffusion: all information of a plaintext symbol is contained in a single cipher text symbol.<br>• Susceptibility to insertions/ modifications: an active interceptor who breaks the algorithm might insert spurious text that looks authentic. |

**Activity 03**

- How many keys are required for secure communication among 500 persons if:

- Symmetric key encryption algorithm is used?
  N*(N-1)/2= (500*499)/2=124,750

- Asymmetric key encryption algorithm is used?
  2N=2*500=1000

**Activity 04**

- Write a program to get the substitution key and the plain text and print the relevant cipher text!

```
#include <stdio.h>
#include <string.h>
#include <time.h>
#include <stdlib.h>

#define swap(a,b) { a=a^b; b=a^b; a=b^a; }

int main() {
char s[] = "abcdefghijklmnopqrstuvwxyz";
unsigned i, c;

srand(time(NULL));
for (i = strlen(s) - 1; i > 0; --i) {
c = rand() % i;
swap(s[c], s[i]);
}
puts(s);
}
```