A seminar on

Cryptography

Presented by

Pratanu Mandal
Dev Gobind Ganguly

JISCE

What is Cryptography?

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Where is cryptography used?

And of course Banking

A Simple Example

Can you tell me what the following means ?

URYYB JBEYQ

A Simple Example

Can you tell me what the following means ?

URYYB JBEYQ

It means

HELLO WORLD

It is obtained by cyclically rotating each letter by 13.

Ex: H => U

E => R and so on.

This simple algorithm is known as **rot-13** or **rotate-13**.

Some Cryptographic Terms

Plaintext	A message in its natural format readable by an attacker.
Ciphertext	Message altered to be unreadable by anyone except the intended recipients.
Key	Sequence that controls the operation and behavior of the cryptographic algorithm.
Keyspace	Total number of possible values of keys in a cryptographic algorithm.

Types of Keys

Symmetric

- Same key for encryption and decryption
- Key distribution problem

Asymmetric

- Mathematically related key pairs for encryption and decryption
- Public and private keys

Hybrid

- Combines strengths of both methods
- Asymmetric distributes symmetric key (session key)
- Symmetric provides bulk encryption

One-time Pad

In cryptography, the one-time pad (OTP) is an encryption technique in which a plaintext is paired with a random secret key (also referred to as a one-time pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition.

One-time Pad (cont ...)

Example: Encryption using One-time Pad

Plaintext : HELLO
Key : XMCKL

```
   H      E      L      L      O      message
   7(H)   4(E)   11(L)  11(L)  14(O)  message
+  23(X)  12(M)  2(C)   10(K)  11(L)  key
=  30     16     13     21     25     message + key
=  4(E)   16(Q)  13(N)  21(V)  25(Z)  message + key (mod 26)
   E      Q      N      V      Z      ciphertext
```

Ciphertext: EQNVZ

Stream Cipher

A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream).

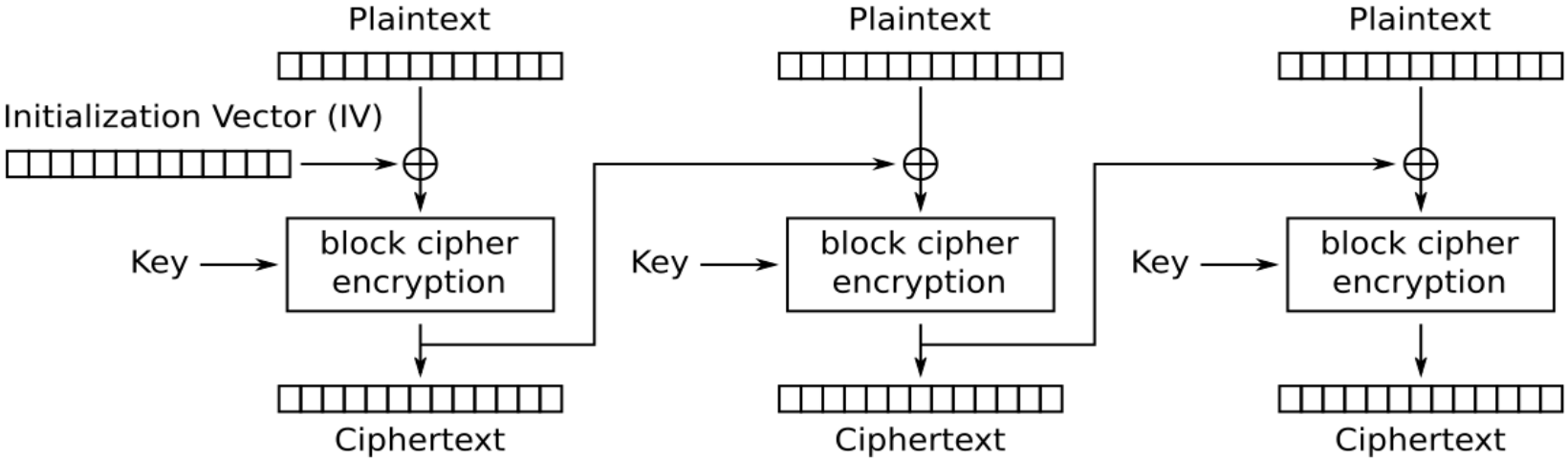
In practice, a digit is typically a bit and the combining operation an exclusive-or (XOR).

Block Cipher

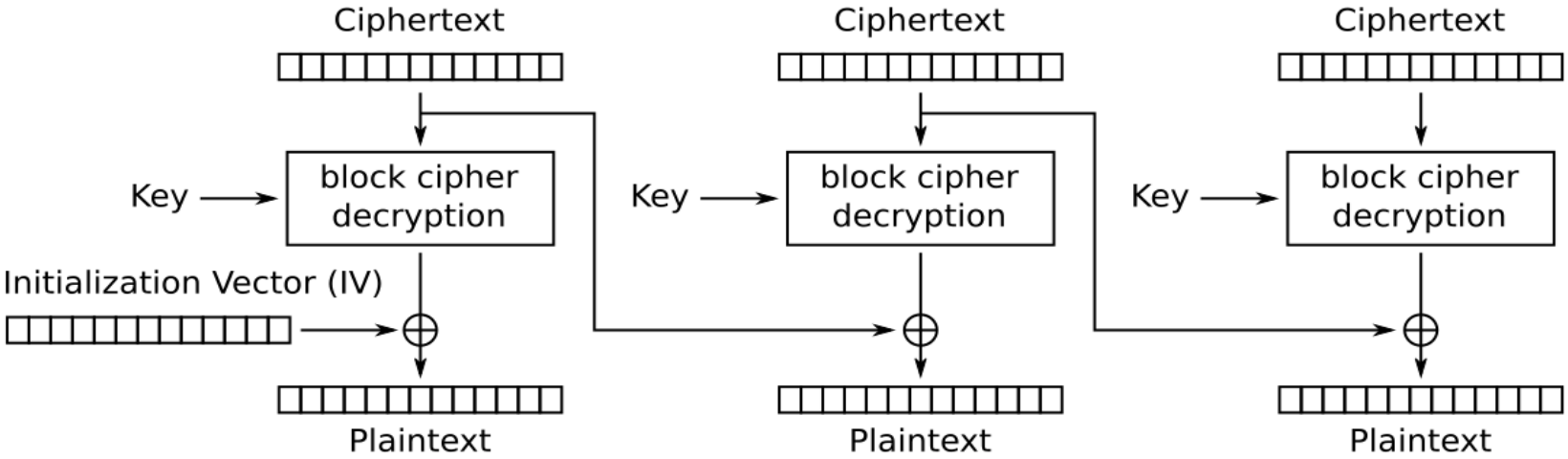
A block cipher is a method of encrypting plaintext (to produce ciphertext) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time.

Initialization Vector

In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic algorithm that is typically required to be random or pseudorandom.



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Any Questions?