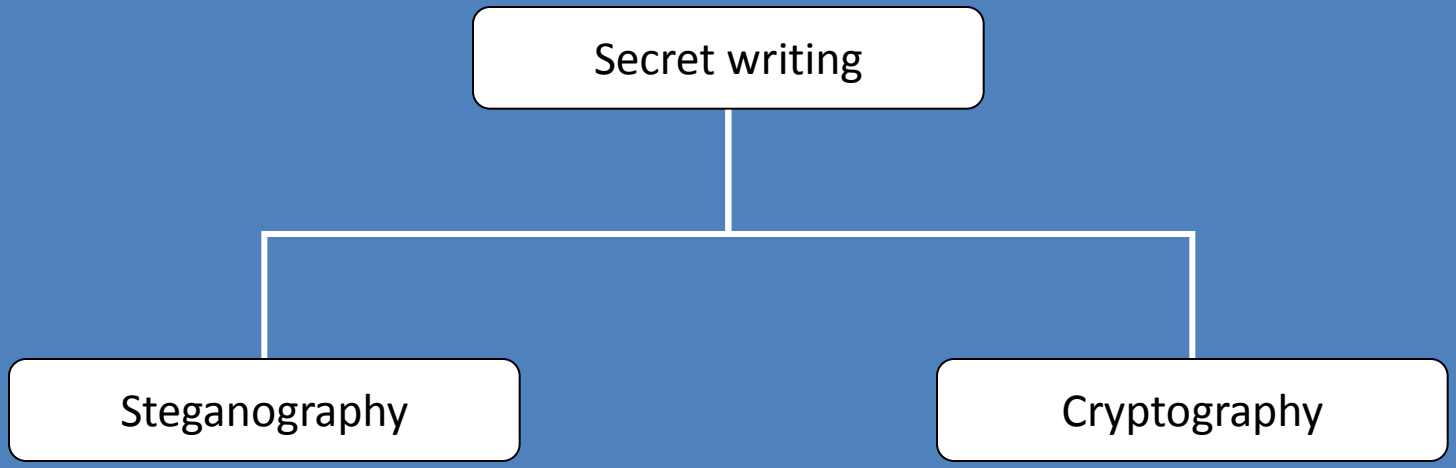
Cryptography

Outlines:

- History
- Basic terminologies
- Symmetric key encryption
- Asymmetric key encryption
- Hashing Structure
- LAB: Encrypting and Decrypting

By: Arash Habibi Lashkari
July - 2010

Types of Secret Writing



Cryptography

- Cryptography deals with creating documents that can be shared secretly over public communication channels

Cryptographic documents are decrypted with the key associated with encryption, with the knowledge of the encryptor

The word cryptography comes from the Greek words: Krypto (secret) and graphein (write)

Cryptography

We will Meet up on next Monday at 12:00 in London Hide Park main entry.

LA KOLE KOUL TP ZV HGTJ LKMTHK zd df jp vxztyh dmso sqkwx zurj plmq.

We will Meet up on next Monday at 12:00 in London Hide Park main entry.

History of Cryptography

- 50 B.C. Julius Caesar uses cryptographic technique
- 400 A.D. Kama Sutra in India mentions cryptographic techniques
- 1250 British monk Roger Bacon describes simple ciphers
- 1466 Leon Alberti develops a cipher disk
- 1861 Union forces use a cipher during Civil War

History of Cryptography

- 1914 World War I – British, French, and German forces use encryption technology
- 1917 William Friedman, Father of U.S. encryption efforts starts a school for teaching cryptanalysis in Illinois
- 1917 AT&T employee Gilbert Vernam invents polyalphabetic cipher
- 1919 Germans develop the Engima machine for encryption

History of Cryptography

- 1937 Japanese design the Purple machine for encryption
- 1942 Navajo windtalkers help with secure communication during World War II
- 1948 Claude Shannon develops statistical methods for encryption/decryption
- 1976 IBM develops DES
- 1976 Diffie – Hellman develop public key / private key cryptography
- 1977 Rivest – Shamir – Adleman develop the RSA algorithm for public key / private key

Steganography

- Steganography is the method of hiding secret messages in an ordinary document

Steganography does not use encryption

Steganography does not increase file size for hidden messages

Example: select the bit patterns in pixel colors to hide the message

Image Steganography

Image in which to hide another image

Image to hide within the other image

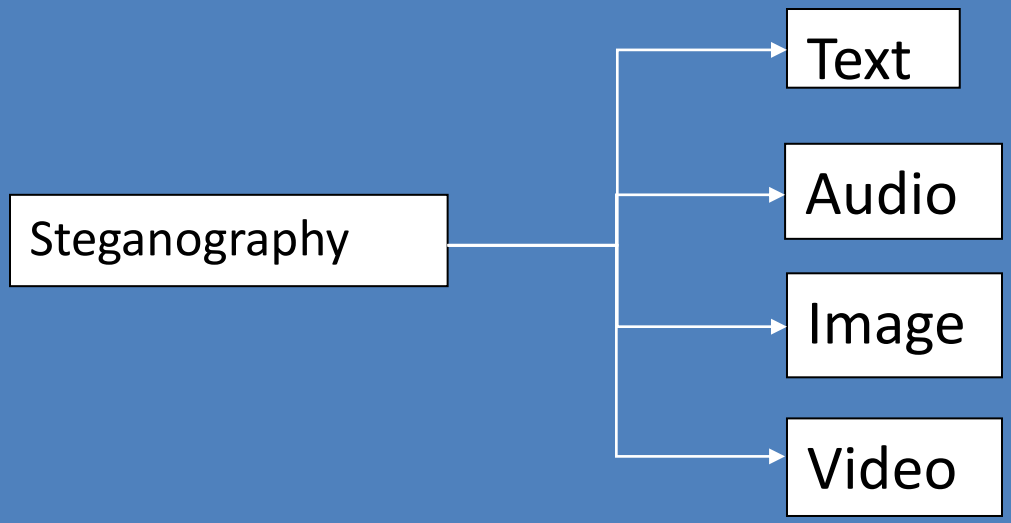
http://www.cl.cam.ac.uk/~fapp2/steganography/image_downgrading/

History of Steganography

- In ancient Greece, for instance a person would chip off wax on a tablet that was wrapped in wax, write a message below the wax then re-apply the wax. To read the message, all the recipient had to do was merely peel off the wax from the tablet.

- Invisible ink was used for the purpose of hiding information written on pieces of paper from the average person during World War II. For the recipient to view the message they would use liquids such as urine, milk, vinegar and fruit juices because when these substances are heated they darken the writing and make it visible to the human eye

Steganography Media



Cryptography

Basic Terminologies in Crypto

- Cryptanalysis deals with finding the encryption key without the knowledge of the encryptor
- Cryptology deals with cryptography and cryptanalysis
- Cryptosystems are computer systems used to encrypt data for secure transmission and storage
- Encryption

  Plain text → Cipher text
- Decryption

  Cipher text → Plain text

Basic Terminologies in Crypto

- Keys are rules used in algorithms to convert a document into a secret document
- Keys are of two types:
  - Symmetric
  - Asymmetric
- A key is symmetric if the same key is used both for encryption and decryption
- A key is asymmetric if different keys are used for encryption and decryption

Basic Terminologies in Crypto

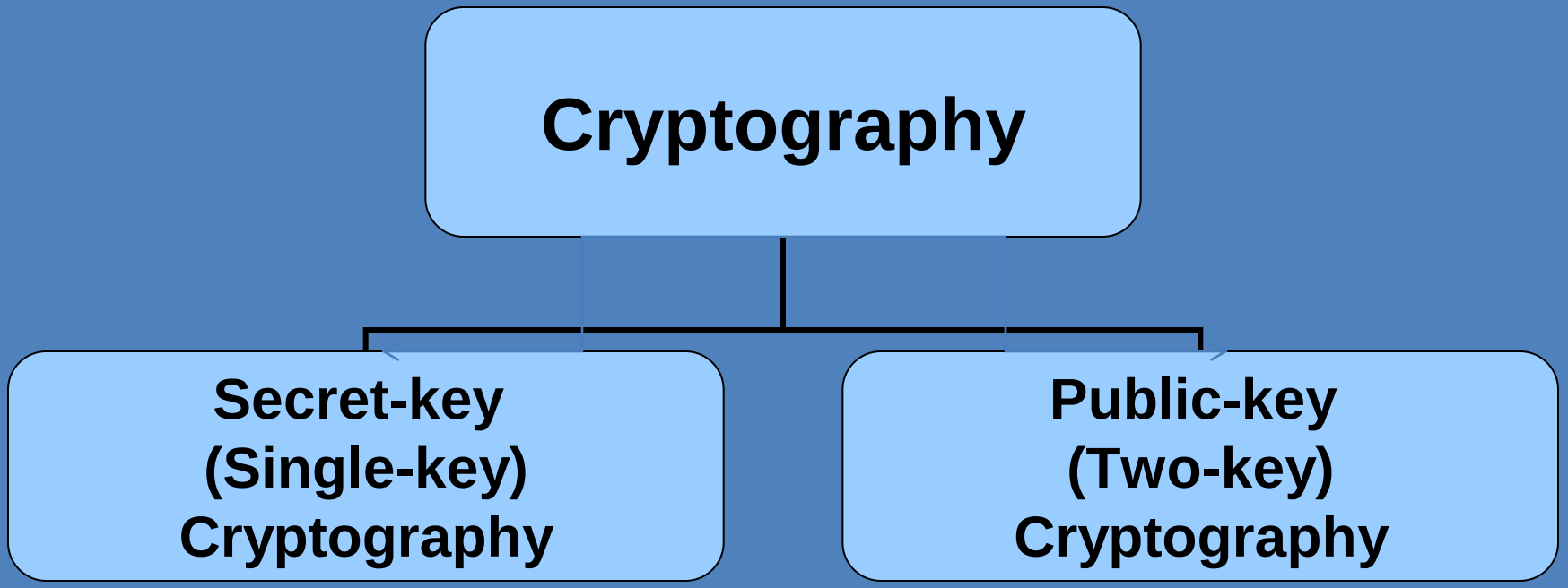
- Examples:
  - Symmetric key methods
    - DES 56-bit
    - Triple DES 128-bit
    - AES 128-bit and higher
    - Blowfish 128-bit and higher
  - Asymmetric key methods
    - RSA (Rivest-Shamir-Adleman of MIT)
    - PGP (Phil Zimmerman of MIT)

Basic Terminologies in Crypto

- Plaintext is text that is in readable form
- Ciphertext results from plaintext by applying the encryption key
- Notations:
  - M: message, C:ciphertext, E:encryption,D: decryption, k: key
  - E(M) = C
  - E(M, k) = C
  - D(C) = M
  - D(C, k) = M

Benefits of Cryptography

- Data secrecy
- Data integrity
- Authentication of message originator
- Electronic certification and digital signature
- Non-repudiation



- A conventional Cryptographic system relies on use of a single piece of private and necessarily secret key.
- Key is known to sender & receiver, but to no others.

- Each user is provided with key material of one's own with a private component & a public component
- The private component must be kept secret for secure communication.

Secret-Key or Symmetric Cryptography

- Alice and Bob agree on an encryption method and a shared ***key***.
- Alice uses the key and the encryption method to ***encrypt*** (or ***encipher***) a message and sends it to Bob.
- Bob uses the same key and the related decryption method to ***decrypt*** (or ***decipher***) the message.

Advantages of Classical Cryptography

- There are some very fast classical encryption (and decryption) algorithms
- Since the speed of a method varies with the length of the key, faster algorithms allow one to use longer key values.
- Larger key values make it harder to guess the key value -- and break the code -- by brute force.

Disadvantages of Classical Cryptography

- ***Requires secure transmission of key value***
- Requires a separate key for each group of people that wishes to exchange encrypted messages (readable by any group member)
  - For example, to have a separate key for each pair of people, 100 people would need 4950 different keys.

Public-Key/Asymmetric Cryptography

- Alice generates a key value (usually a number or pair of related numbers) which she makes public.
- Alice uses her public key (and some additional information) to determine a second key (her ***private key***).
- Alice keeps her private key (and the additional information she used to construct it) secret.

Public-Key Cryptography (continued)

- Bob (or Carol, or anyone else) can use Alice's public key to encrypt a message for Alice.
- Alice can use her private key to decrypt this message.
- No-one without access to Alice's private key (or the information used to construct it) can easily decrypt the message.

An Example: Internet Commerce

- Bob wants to use his credit card to buy some brownies from Alice over the Internet.
- Alice sends her public key to Bob.
- Bob uses this key to encrypt his credit-card number and sends the encrypted number to Alice.
- Alice uses her private key to decrypt this message (and get Bob's credit-card number).

Hybrid Encryption Systems

- All known public key encryption algorithms are much slower than the fastest secret-key algorithms.
- In a ***hybrid*** system, Alice uses Bob's public key to send him a secret shared ***session key***.
- Alice and Bob use the session key to exchange information.

Internet Commerce (continued)

- Bob wants to order brownies from Alice and keep the ***entire transaction*** private.
- Bob sends Alice his public key.
- Alice generates a session key, encrypts it using Bob's public key, and sends it to Bob.
- Bob uses the session key (and an agreed-upon symmetric encryption algorithm) to encrypt his order, and sends it to Alice.

Digital Signatures

- Alice applies a (publicly known) ***hash function*** to a document that she wishes to "sign." This function produces a ***digest*** of the document (usually a number).
- Alice then uses her ***private*** key to "encrypt" the digest.
- She can then send, or even broadcast, the document with the encrypted digest.

Digital Signature Verification

- Bob uses Alice's ***public*** key to "decrypt" the digest that Alice "encrypted" with her private key.
- Bob applies the hash function to the document to obtain the digest directly.
- Bob compares these two values for the digest. If they match, it proves that Alice signed the document and that no one else has altered it.

Block Ciphers

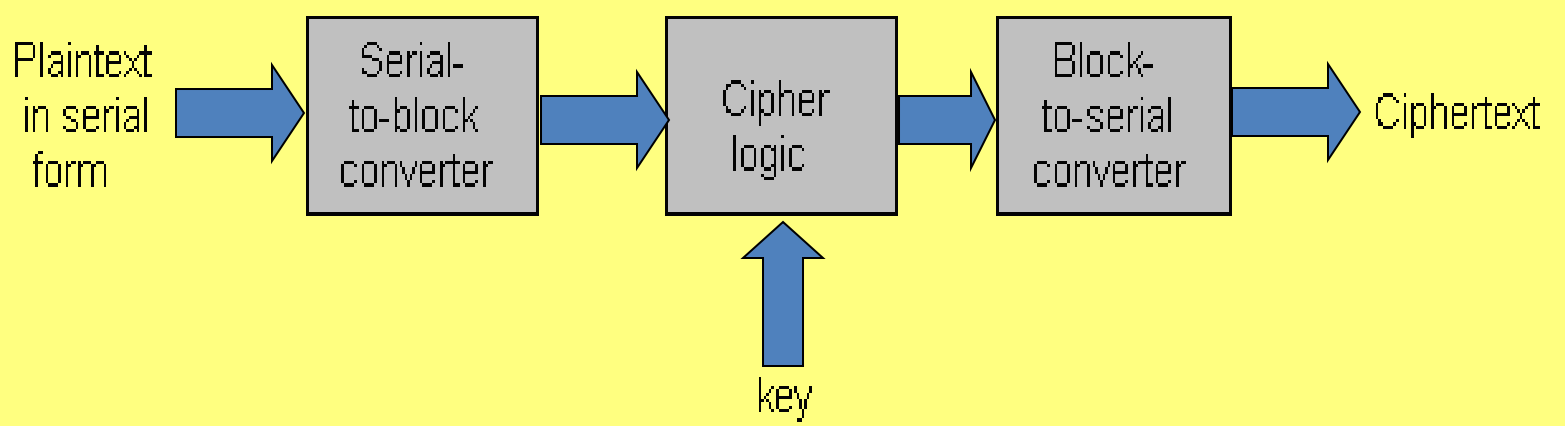


Figure 3: Block diagram of a block cipher

- **Block ciphers are normally designed in such a way that a small change in an input block of plaintext produces a major change in the resulting output.**
- **This error propagation property of block ciphers is valuable in authentication in that it makes it improbable for an enemy cryptanalyst to modify encrypted data, unless knowledge of key is available.**

Stream ciphers

- **Whereas block ciphers operate on large data on a block-by-block basis, stream ciphers operate on individual bits.**

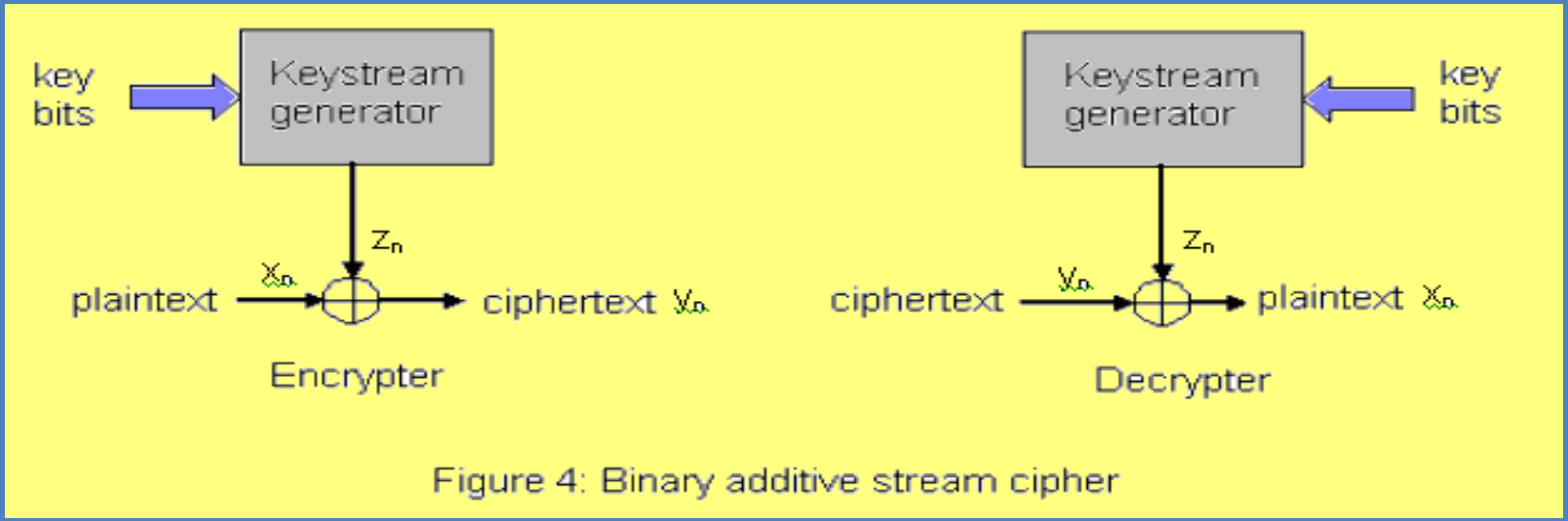


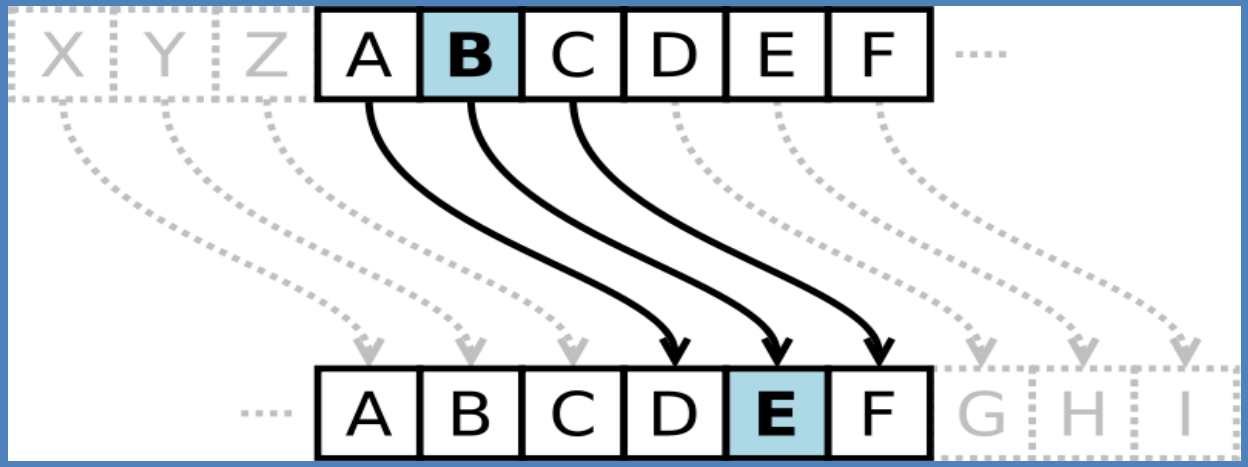
Figure 4: Binary additive stream cipher

Let x_n -> Plaintext bit; y ->ciphertext bit; z ->keystream bit at n^{th} instant

For encryption: $y_n = x_n \oplus z_n$, n=1, 2, …, N

For decryption: $x_n = y_n \oplus z_n$, n=1, 2, …, N

Substitution Ciphers



Encryption algorithm

Substitute top row character with bottom row character

Decryption algorithm

Substitute bottom row character with top row character

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

Key

Caesar Ciphers

More formally:

Encrypt(Letter, Key) = (Letter + Key) (mod 26)

Decrypt(Letter, Key) = (Letter - Key) (mod 26)

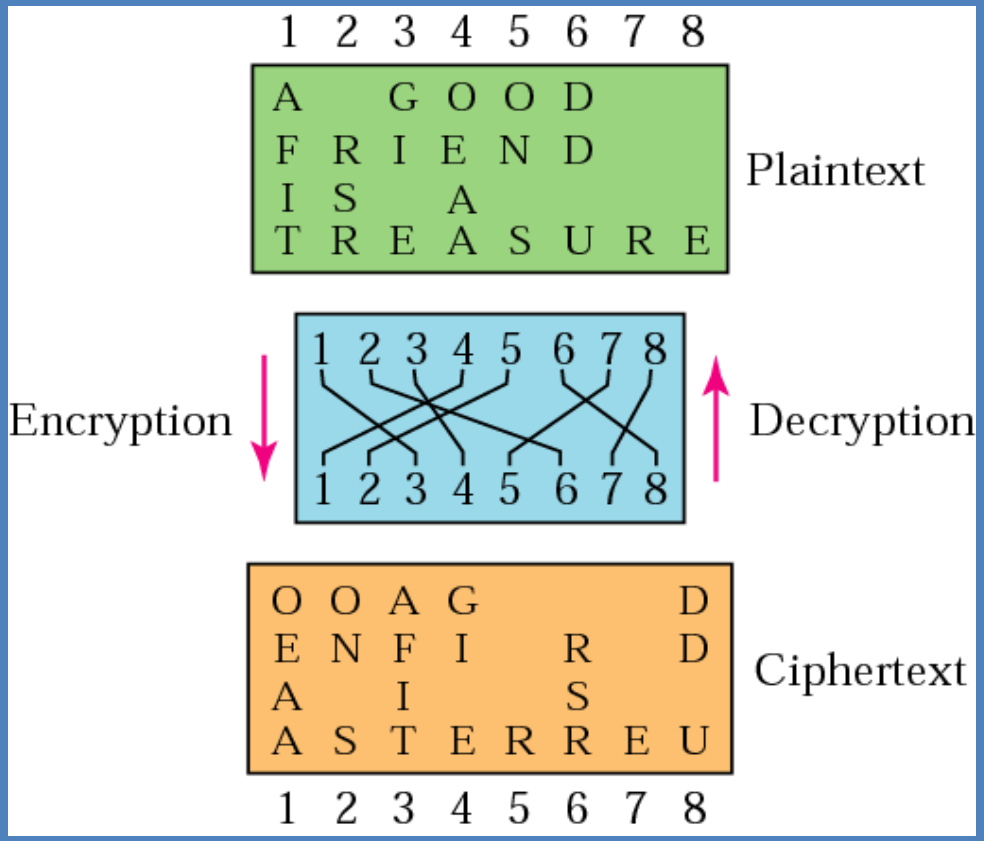
Encrypt(“NIKITA”, 3) = “QLNLWD”

Decrypt(“QLNLWD”, 3) = “NIKITA”

Transposition cipher

- The plaintext is divided into groups of fixed period d & the same permutation is applied to each group.

- The particular permutation rule being determined by the secret key.



Vigenere cipher

- A different caesar cipher per letter

  MORESECURETHANCAESAR (Ciphertext)

  + SECRETSECRETSECRETSE (Key)

  = FTUWXYVZUWYBTSFSJMTW

  – M (13) + S (19) = F (6) mod 26
  – O (15) + E (5) = T (20) mod 26
  – …

Crypto Attacks

- *Ciphertext only* attack:
  - Recover plaintext knowing only the ciphertext
- Ciphertext:
  - **HSPAA SLRUV DSLKN LPZHK HUNLY VBZAO PUN**

Brute force

- Ciphertext = **IGKYGXOYOTYKIAXK**
  - Decrypt(IGKYGXOYOTYKIAXK, 1) = HFJXFWNXNSXJHZWJ
  - Decrypt(IGKYGXOYOTYKIAXK, 2) = GEIWEVMWMRWIGYVI
  - Decrypt(IGKYGXOYOTYKIAXK, 3) = FDHVDULVLQVHFXUH
  - Decrypt(IGKYGXOYOTYKIAXK, 4) = ECGUCTKUKPUGEWTG
  - Decrypt(IGKYGXOYOTYKIAXK, 5) = DBFTBSJTJOTFDVSF
  - Decrypt(IGKYGXOYOTYKIAXK, 6) = CAESARISINSECURE

Questions

- One group Using Substitution and Transposition Cipher and make Cipher Text
- Other group try to find the Plaintext