Security and Applications

Symmetric Key Cryptography

Attacks, Services and Mechanisms

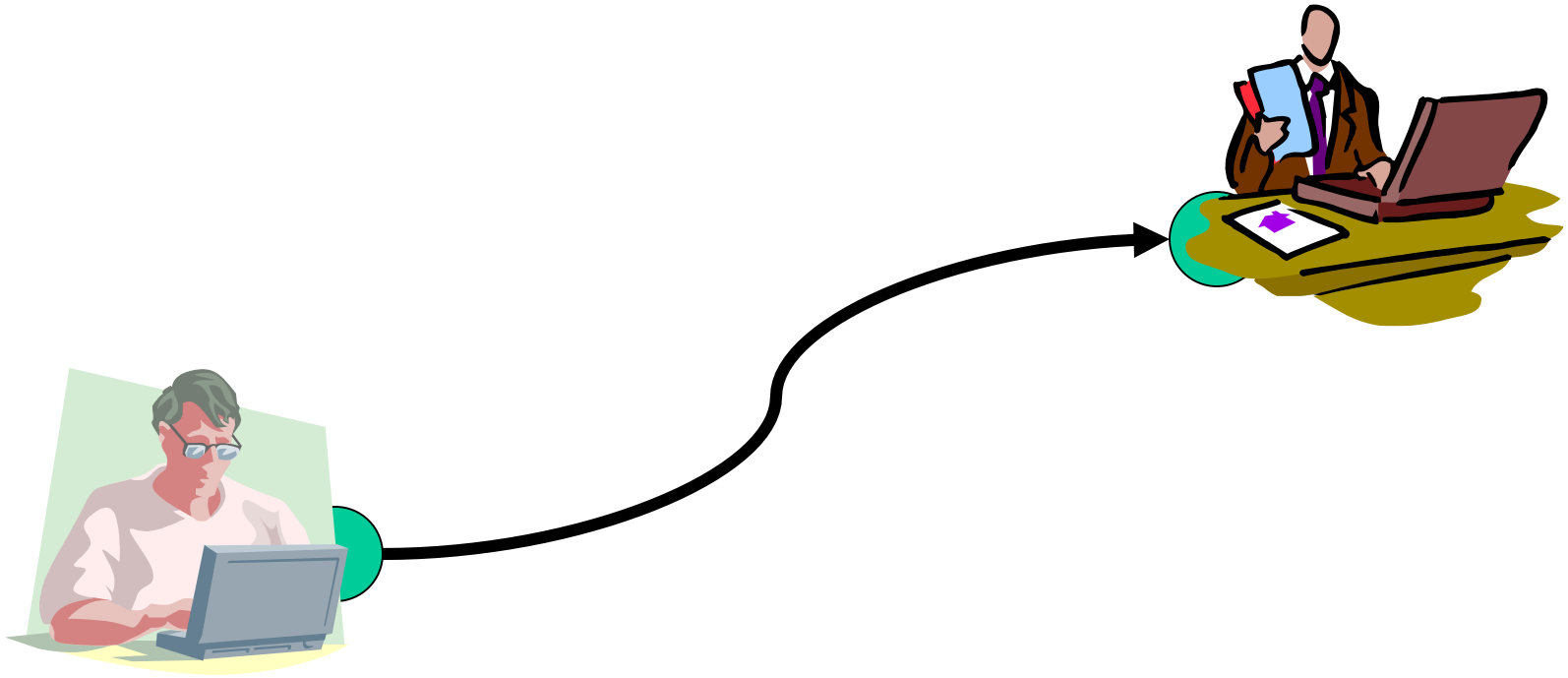
- **Security Attacks**
  - Action compromises the information security
- **Security Services**
  - Security of data processing and transferring
- **Security mechanism**
  - Detect, prevent and recover from a security attack

How security of systems can be compromised?

Attacks

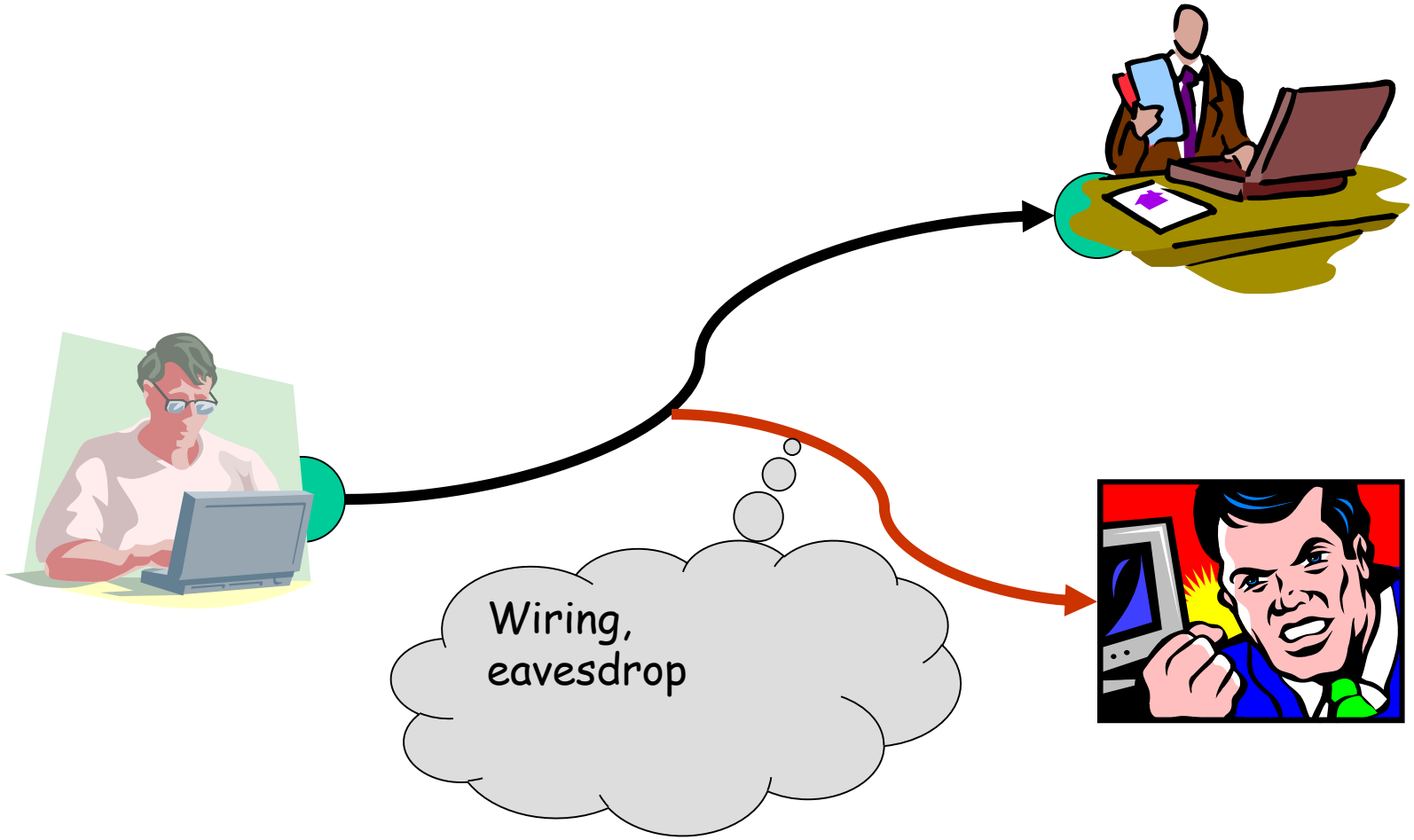
- Malware
- Cybersquatting
- Phishing
- Cyber vandalism
- Masquerading or spoofing
- Denial of Service

Information Transferring

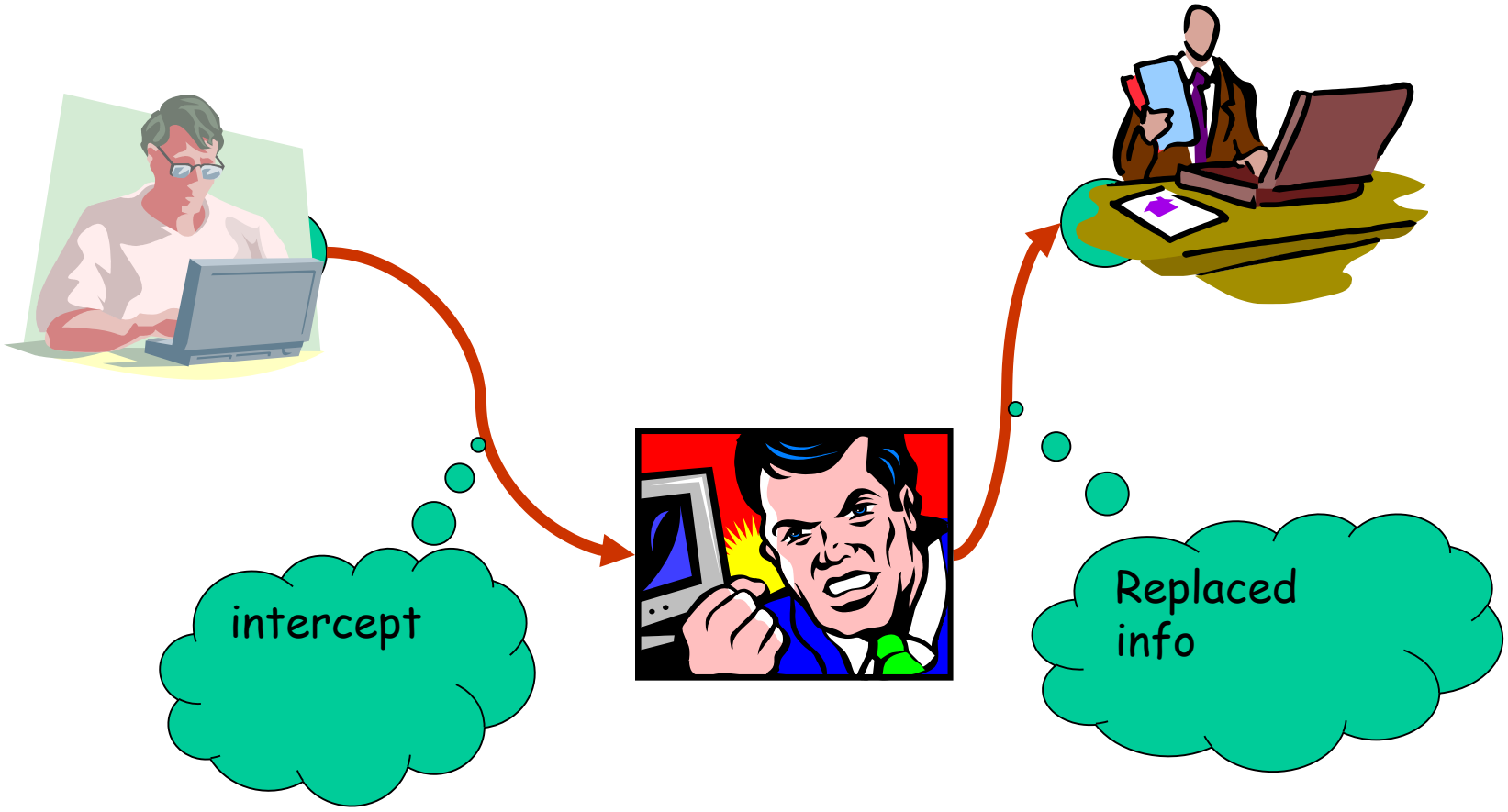


How an adversary can compromise communication

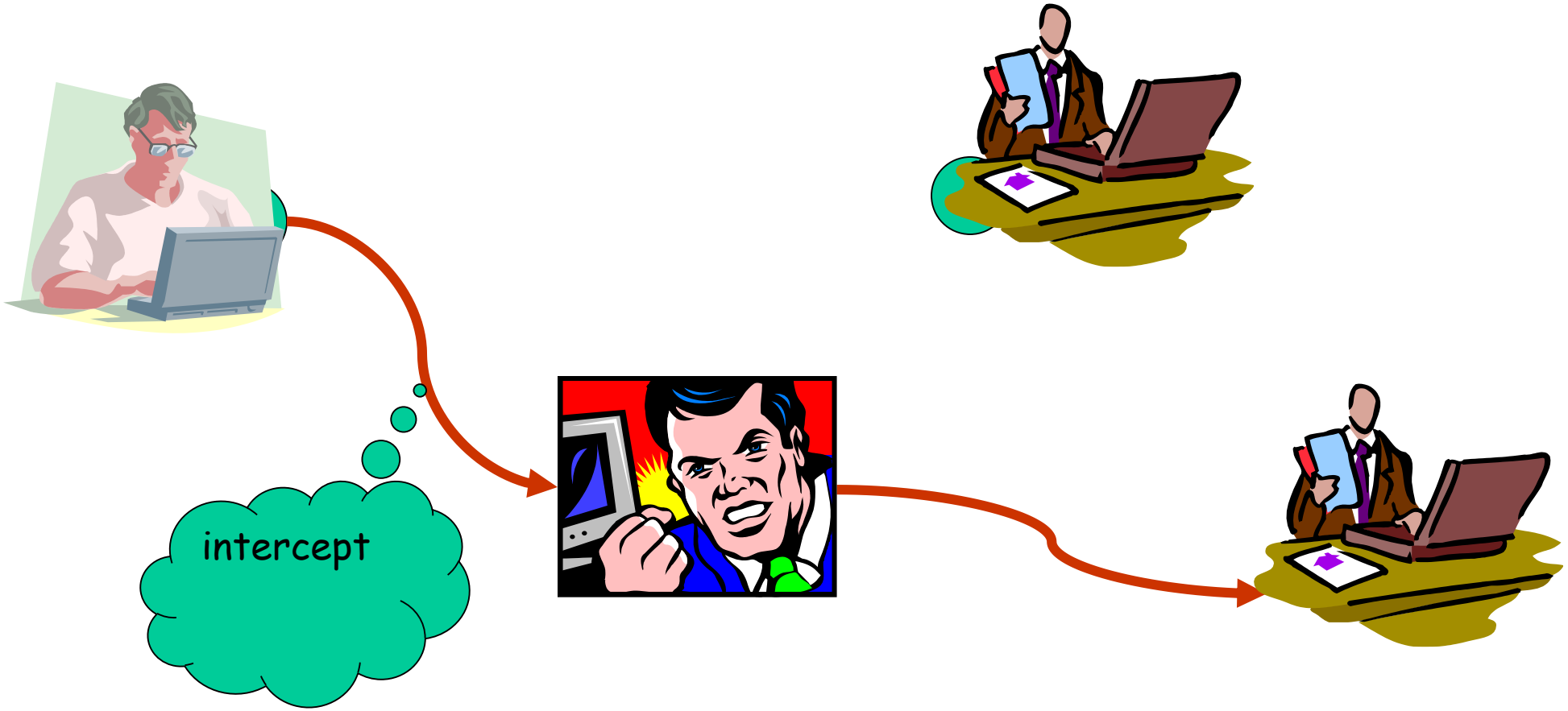
Attack: Interception



Attack: Modification



Attack: change of recipient

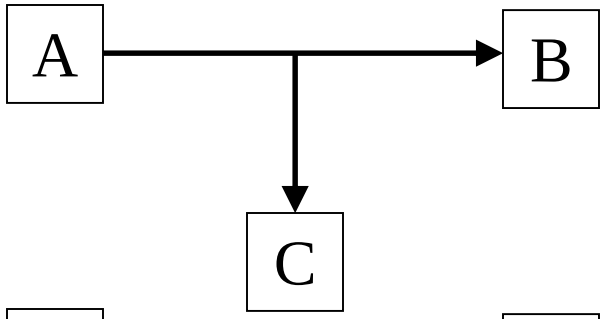


Attack: Fabrication

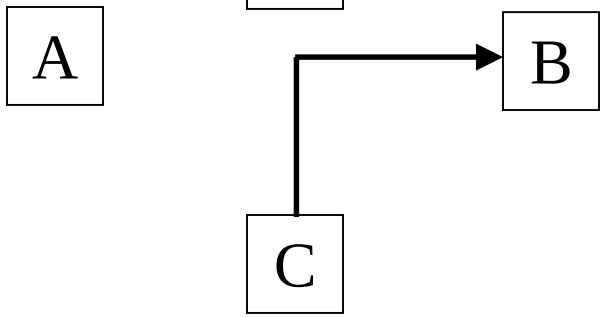
Also called impersonation

Information Transfer: Security Services

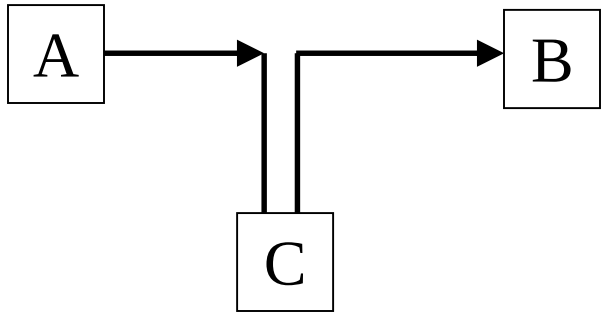
Confidentiality



Authenticity



Integrity



Secure Communication

1. Confidentiality (Secrecy)
   - Only intended receiver understands the message
2. Authentication
   - Sender and receiver need to confirm each others identity
3. Message Integrity
   - Ensure that their communication has not been altered, either maliciously or by accident during transmission
4. Non-repudiation:
   - the sender should not be able to deny sending the message.

Designing Service

1. Design an algorithm
2. Generate secret information
3. Develop methods for the distribution and sharing of secret information
4. Specify a protocol to be used

Attacks

- Passive attacks
  - Interception
    - Release of message contents
    - Traffic analysis
- Active attacks
  - Interruption, modification, fabrication
    - Masquerade
    - Replay
    - Modification
    - Denial of service

Attack Surfaces

- System
  - Open ports
  - Firewall
  - Code processing email,XML,docs
  - Interfaces, SQL
  - Employee
- Software
  - Application
  - OS code
  - Webserver software
- Human
  - Personnel
  - Outsiders
  - Social Engineering
  - Human Error

Enabling Secure Communication

- Code
- Steganography
- Cryptography

Code	Meaning
Hat	boat
Has been sent	arrives
Friday	tomorrow

Steganography

- Conceal the existence of message
  - Character marking
  - Invisible ink
  - Typewriter correction ribbon

Steganography

- Least significant bits of picture frames
  - 2048x3072 pixels with 24-bits RGB info
  - Able to hide 2.3M message
- Drawbacks
  - Large overhead
  - Virtually useless if system is known

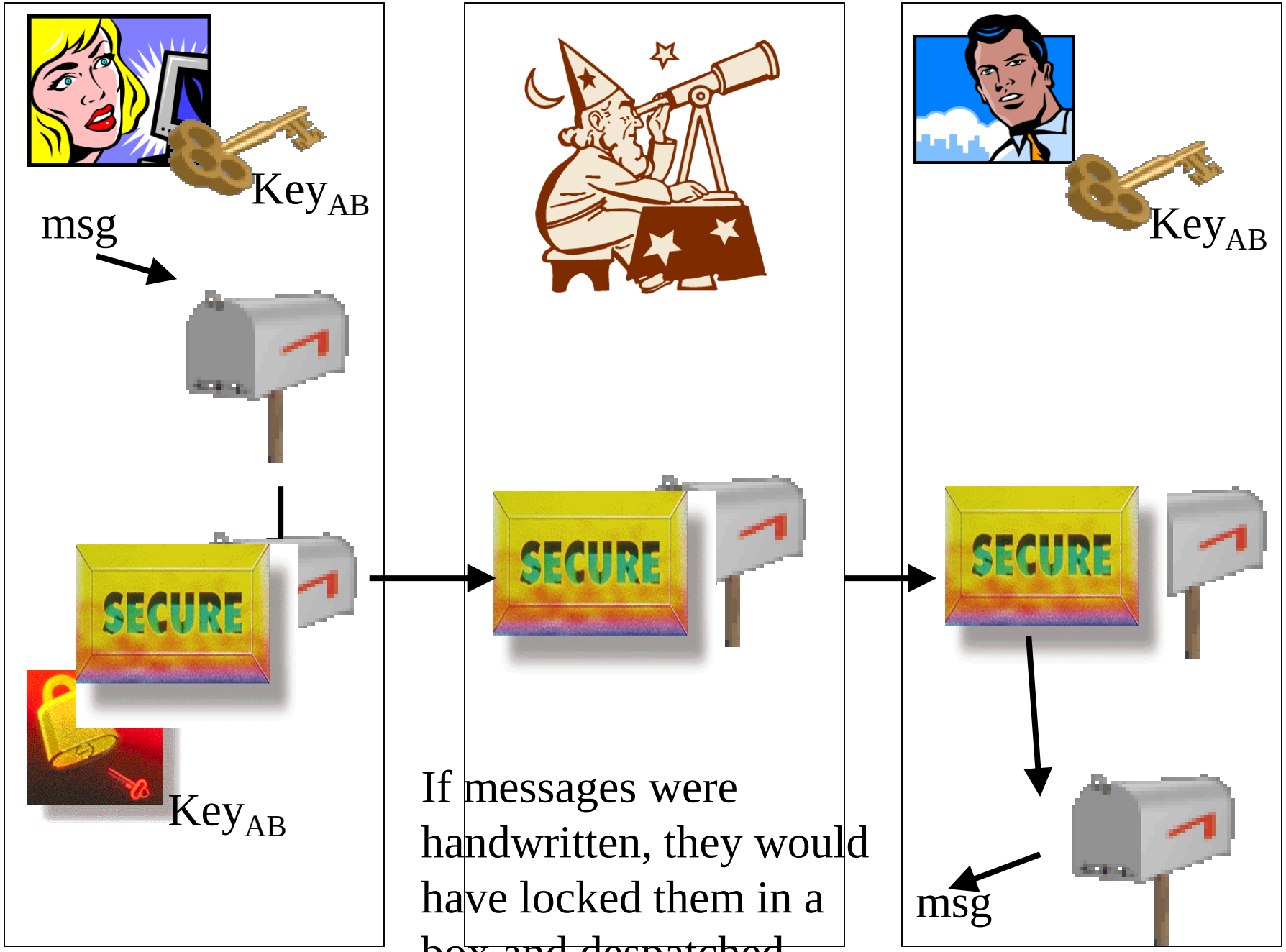
Cryptography

- **Cryptography** (from Greek *kryptós*, "hidden", and *gráphein*, "to write") is, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge — the art of *encryption*.
- **Secret (crypto-) writing (-graphy)**

msg

msg

Alice and Bob do not want anyone in the middle to know about their messages



If messages were handwritten, they would have locked them in a box and despatched

Cryptography Algorithms

- A crypto algorithm transforms an intelligible message into one that is unintelligible, and then retransforming that message back to its original form, so that:-
  - Conceal the context of some message from all except the sender and recipient (privacy or secrecy), and/or
  - Verify the correctness of a message to the recipient (**authentication**)

Crypto-graphy, -analysis, -logy

- The study of how to circumvent the use of cryptography is called *cryptanalysis*, or *codebreaking*.
- Cryptography and cryptanalysis are sometimes grouped together under the umbrella term **cryptology**, encompassing the entire subject.

Cryptanalysis: Strength of Encryption (lock)

Unconditionally secure

- If it is impossible determine uniquely P from C, no matter how much ciphertext is available.

Practically Unconditionally secure

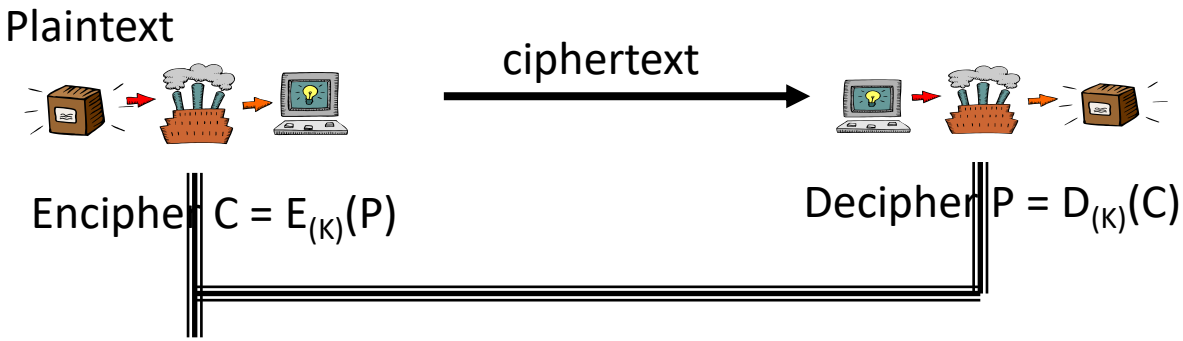
- Cost of breaking cipher exceeds the value of information.
- The time required is very high (> age of info or universe)

Computational security

- Given limited computing resources, the cipher cannot be broken in a reasonable time

Cryptography

- It has two main Components:
  1. Encryption-Decryption
     - Practice of hiding messages so that they can not be read by anyone other than the intended recipient



  2. Authentication & Integrity
     - Ensuring that users of data/resources are the persons they claim to be and that a message has not been surreptitiously altered

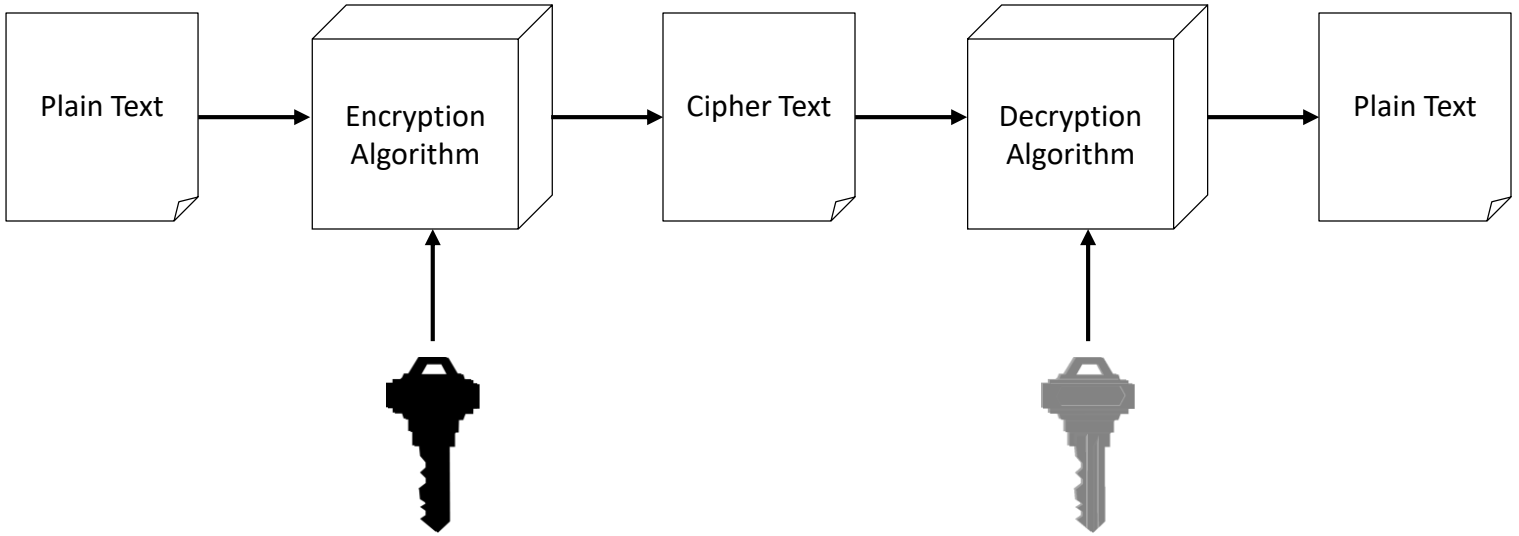
Ingredients of Cryptographic System

- **Plaintext**
  - The original intelligible message
- **Ciphertext**
  - The transformed message
- Message
  - Is treated as a non-negative integer hereafter
- **Cipher**
  - An algorithm for transforming an intelligible message into unintelligible by transposition and/or substitution
- **Key**
  - Some critical information used by the cipher, known only to the sender & receiver
- **Encipher** (encode)
  - The process of converting plaintext to ciphertext
- **Decipher** (decode)
  - The process of converting ciphertext back into plaintext

Encryption

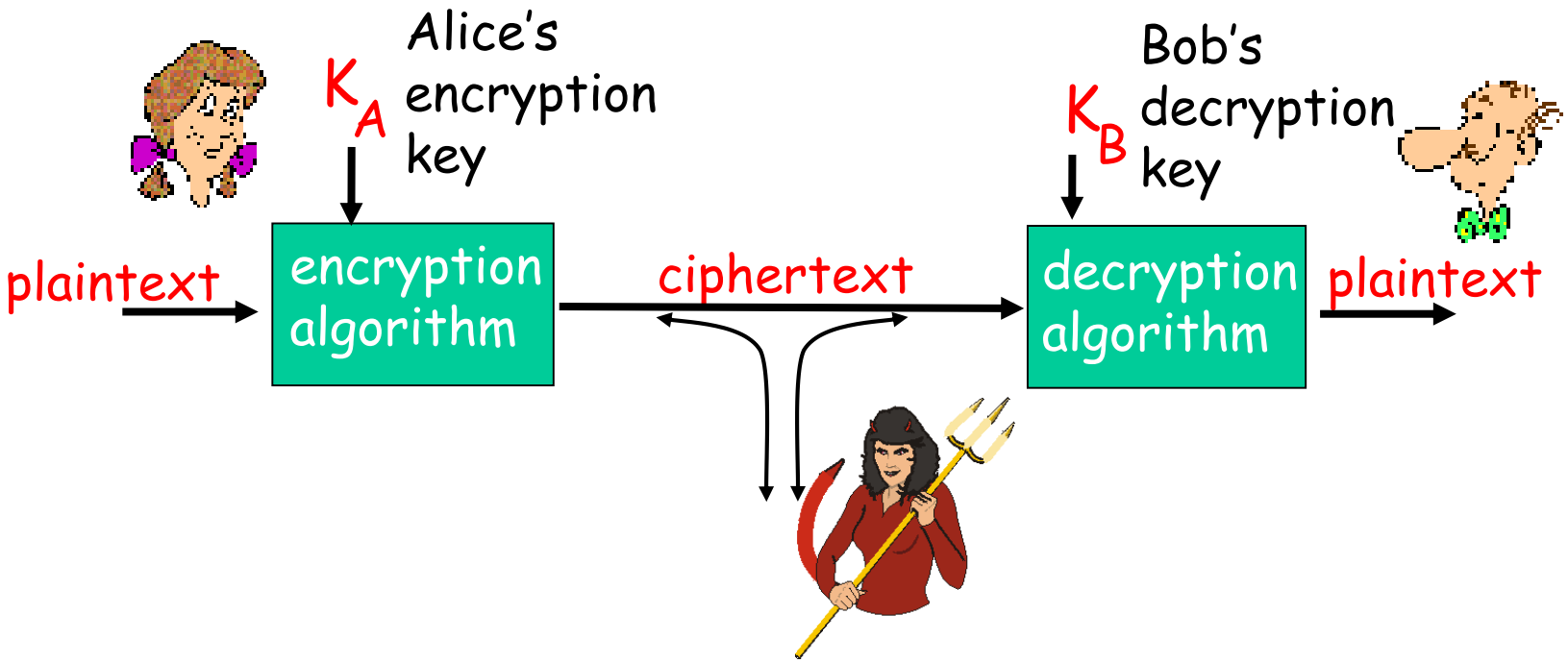
Cipher

- Cipher is a method for encrypting messages



- Encryption algorithms are standardized & published

The language of cryptography



symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret* (private)

Basic Concepts

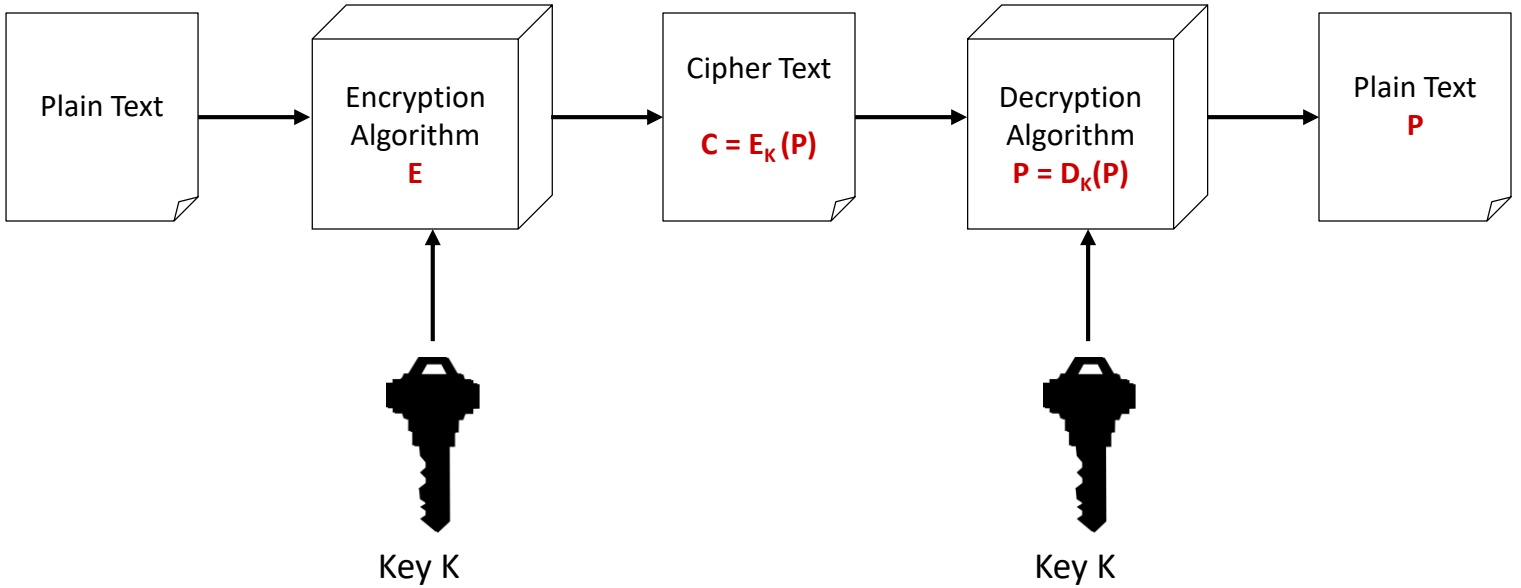
- *cipher*
  - an algorithm for encryption and decryption. The exact operation of ciphers is normally controlled by a key — some secret piece of information that customizes how the ciphertext is produced
- *Protocols*
  - specify the details of how ciphers (and other cryptographic primitives) are to be used to achieve specific tasks.
  - A suite of protocols, ciphers, key management, user-prescribed actions implemented together as a system constitute a *cryptosystem*

Classical Cryptographic Techniques

- Two basic components of classical ciphers:
  - **Substitution:** letters are replaced by other letters
  - **Transposition:** letters are arranged in a different order
- These ciphers may be:
  - **Monoalphabetic**: only one substitution/ transposition is used, or
  - **Polyalphabetic:** where several substitutions/ transpositions are used

Symmetric Encryption

- Key is the same for encryption and decryption



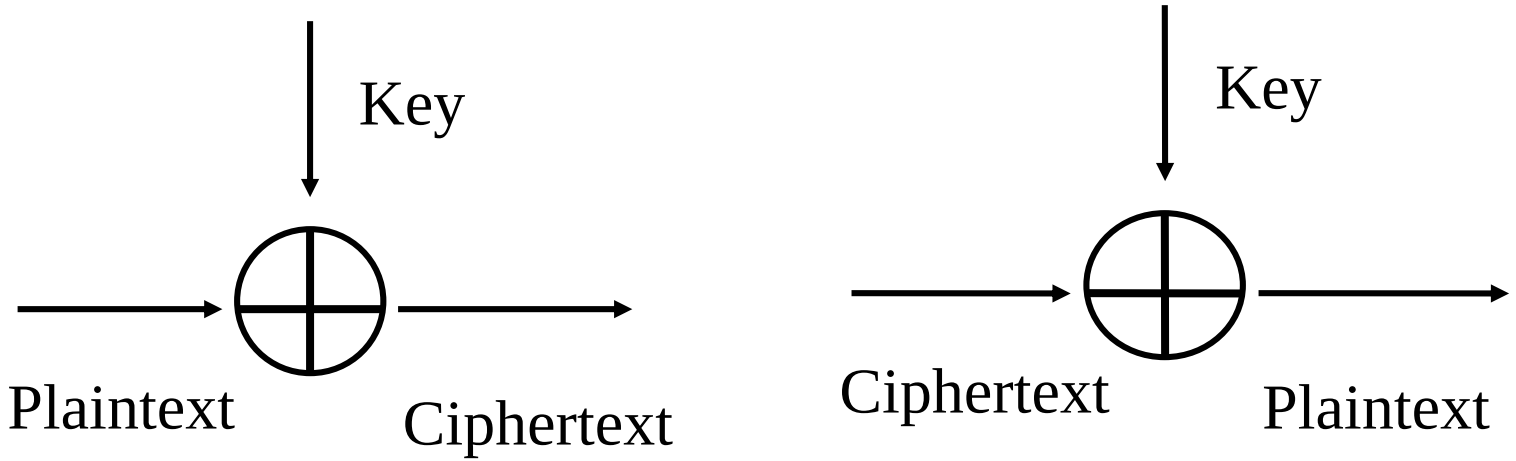
Types of Symmetric Algorithms

- Types:
  1. Block Ciphers
     - Encrypt data one block at a time (typically 64 bits, or 128 bits)
     - Used for a single message
  2. Stream Ciphers
     - Encrypt data one bit or one byte at a time
     - Used if data is a constant stream of information

Stream ciphers

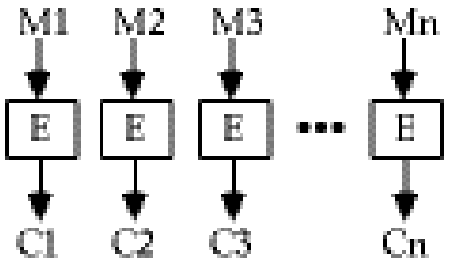
- **Stream ciphers**
  - The most famous: **Vernam cipher**
  - Invented by Vernam, (AT&T, in 1917)
  - Process the message bit by bit (as a stream)
  - Simply add bits of message to random key bits
- Examples
  - A well-known stream cipher is RC4;
  - others include: A5/1, A5/2, Chameleon, FISH, Helix. ISAAC, Panama, Pike, SEAL, SOBER, SOBER-128 and WAKE.
- Usage
  - Stream ciphers are used in applications where plaintext comes in quantities of unknowable length - for example, a secure wireless connection

Stream Cipher



Block Ciphers

- The message is broken into blocks,
  - Each of which is then encrypted
  - (Like a substitution on very big characters - 64-bits or more)



Substitution Cipher

Caesar Cipher

Cleartext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v

hello  KHOOR

Mathematical Model

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19
Cleartext	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Ciphertext	d	e	f	G	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22

- Encryption $E_{(k)}$: $i \rightarrow i + k \bmod 26$
- Decryption $D_{(k)}$: $i \rightarrow i - k \bmod 26$

Exercise

Caesar Cipher

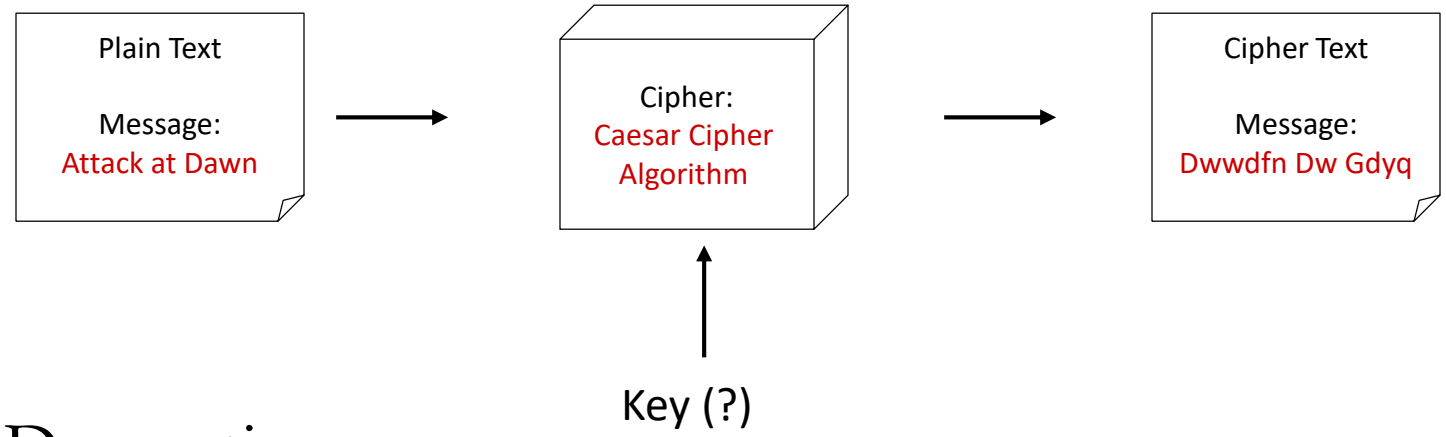
Let us try to encrypt the message

–Attack at Dawn

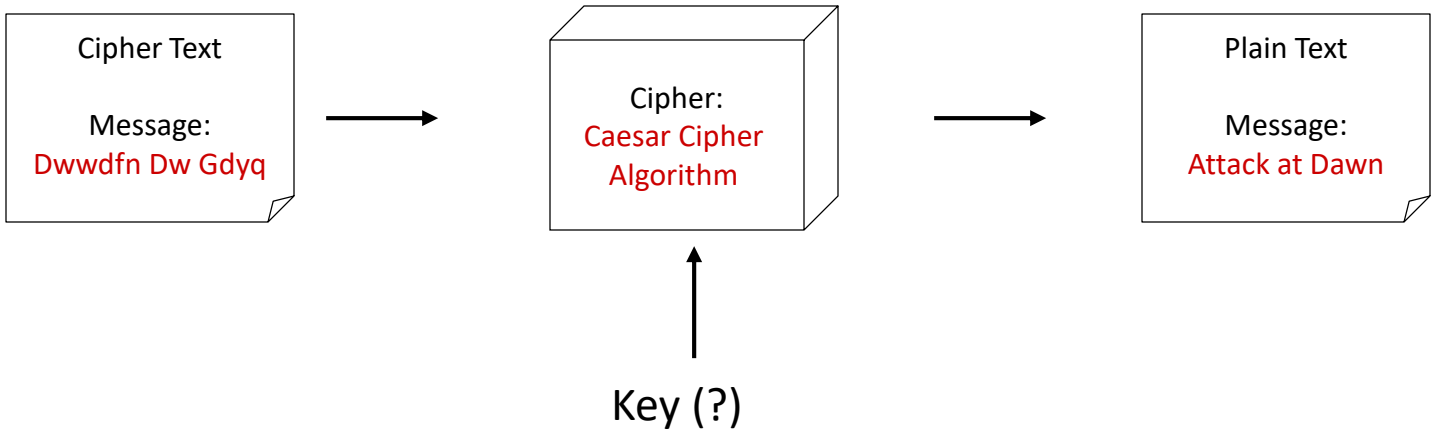
Substitution Ciphers

Caesar Cipher

Encryption



Decryption



How good is this method?

Mono-alphabetic Substitution Cipher

- The key space: all permutations of Σ = {A, B, C, …, Z}
- Encryption given a key π:
  - each letter X in the plaintext P is replaced with $\pi(X)$
- Decryption given a key π:
  - each letter Y in the cipherext P is replaced with $\pi^{-1}(Y)$

Example:

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

BECAUSE → AZDBJSZ

Q: How hard to break this simple cipher?:

- brute force (how hard?)
- other?

Symmetric key cryptography

substitution cipher: substituting one thing for another

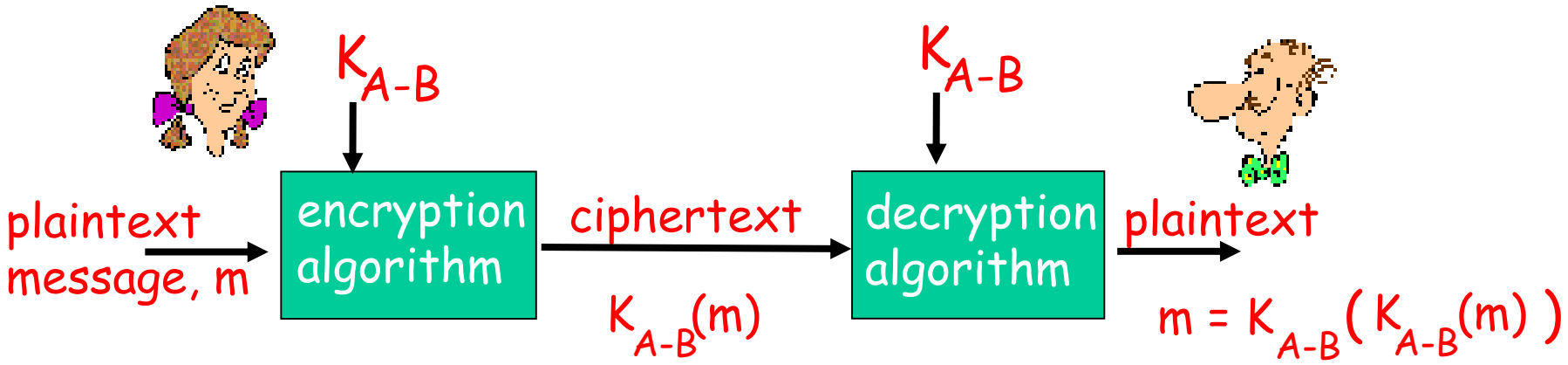
- monoalphabetic cipher: substitute one letter for another

```
plaintext:   abcdefghijklmnopqrstuvwxyz
                ↓                    ↓
key:         mnbvcxzasdfghjklpoiuytrewq
```

E.g.:

```
Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc
```

Symmetric key cryptography



symmetric key crypto: Bob and Alice share know same (symmetric) key: K_{A-B}

e.g., key is knowing substitution pattern in mono alphabetic substitution cipher

- Q: how do Bob and Alice agree on key value?

Key Management

- Using secret channel
- Encrypt the key
- Key Agreement
- Third trusted party
- The sender and the receiver generate key
  - The key must be same
  - We will talk more about how we can generate keys for two parties who are "unknown" of each other before, and want secure communication

Adversarial Goals

- Recover the message
- Recover the secret key
  - Thus also the message
- Thus the number of keys possible must be large!

Cryptanalysis

Techniques

- Cryptanalysis is the process of breaking an encryption code
  - Tedious and difficult process
- Several techniques can be used to deduce the key
  - Attempt to deduce the key, in order to break subsequent messages easily
  - Attempt to recognize patterns in encrypted messages
  - Attempt to infer some meaning without even breaking the encryption, such as noticing an unusual frequency of communication or determining something by whether the communication was short or long
  - Attempt to find weaknesses in the implementation or environment of use of encryption.

Cryptanalysis: Strength of Encryption (lock)

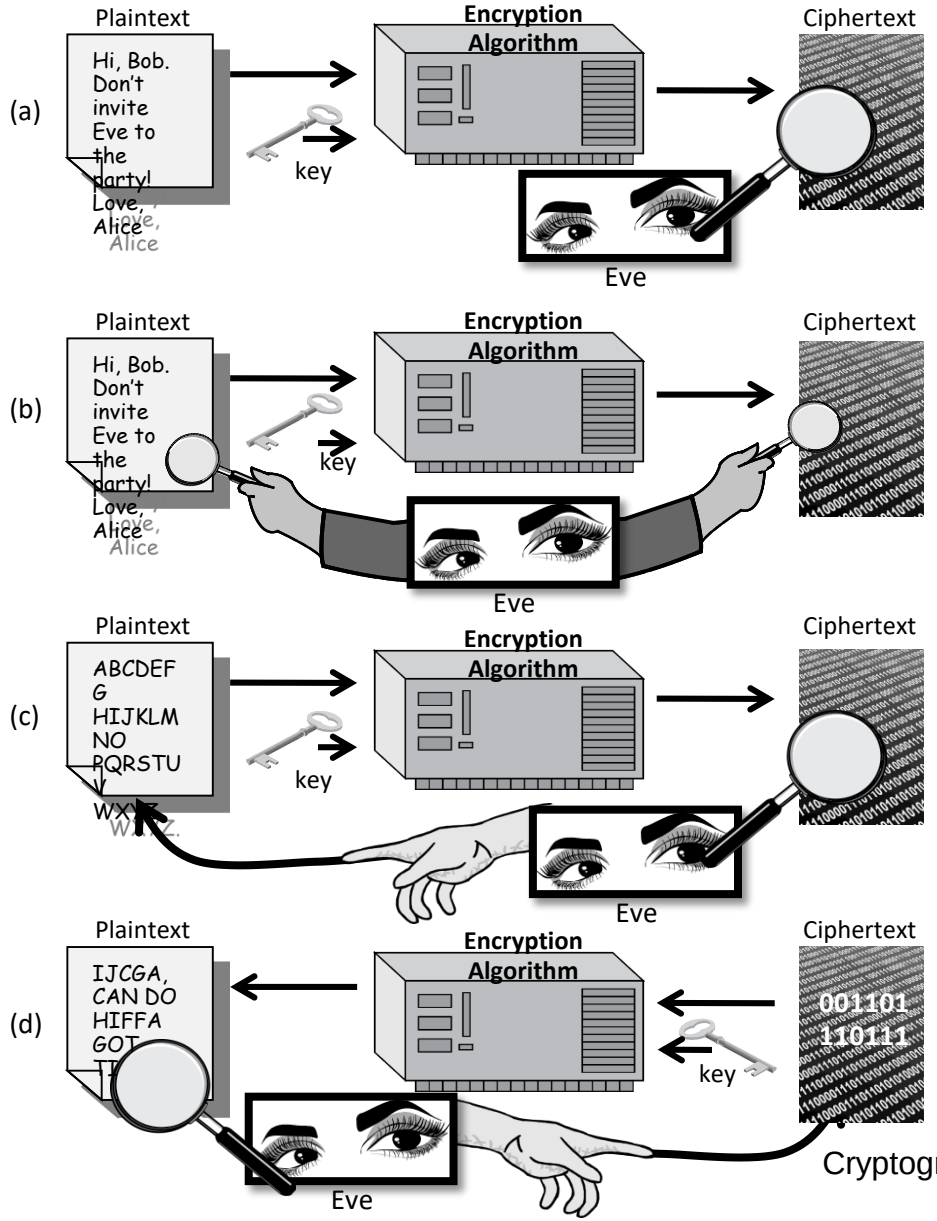
- Attack Model
  - Some knowledge of characteristics of plain text
  - Some plain-text – cipher-text pairs
- Adversarial Goal
  - Complete break
  - Weaker goals
    - probabilistic decrypt
    - partial information about PT
    - Information from CT analysis
- Nature of the algorithm
  - Possibility to try different keys until success (on average half of all possible keys)

Attack Models

- Ciphertext only
  - Algorithm, ciphertext
- Known plaintext
  - Algorithm, ciphertext, plaintext-ciphertext pair
- Chosen plaintext
  - Algorithm, ciphertext, chosen plaintext and its ciphertext
- Chosen ciphertext
  - Algorithm, ciphertext, chosen ciphertext and its plaintext

Attacks

- Attacker may have
  a) collection of ciphertexts (ciphertext only attack)
  b) collection of plaintext/ciphertext pairs (known plaintext attack)
  c) collection of plaintext/ciphertext pairs for plaintexts selected by the attacker (chosen plaintext attack)
  d) collection of plaintext/ciphertext pairs for ciphertexts selected by the attacker (chosen ciphertext attack)



Analysis of Caesar Cipher

- Encryption and Decryption algorithms known
- Only 25 keys to try
- Language of plaintext and ciphertext known, recognizable, with well known characteristics
- Both C and P share the same statistical characteristics.

Modular Arithmetic Cipher

- Use a more complex equation to calculate the ciphertext letter for each plaintext letter
- $E_{(a,b)} : i \rightarrow a*i + b \bmod 26$
  - Need gcd(a,26) = 1
  - Otherwise, not reversible
  - So, $a \neq 2, 13, 26$
  - Caesar cipher: a=1

Cryptanalysis of Modular Arithmetic Cipher

- Key space: *12*26*
  - Brute force search
- Use letter frequency counts to guess a couple of possible letter mappings
  - frequency pattern not produced just by a shift
  - use these mappings to solve 2 simultaneous equations to derive above parameters

Attacks

- Recover the message
- Recover the secret key
  - Thus also the message
- Thus the number of keys possible must be large!

Symmetric Encryption

Key Strength

- Strength of algorithm is determined by the size of the key
  - The longer the key the more difficult it is to crack
- Key length is expressed in bits
  - Typical key sizes vary between 48 bits and 448 bits
- Set of possible keys for a cipher is called key space
  - For 40-bit key there are 2^{40} possible keys
  - For 128-bit key there are 2^{128} possible keys
  - Each additional bit added to the key length doubles the security
- To crack the key the hacker has to use brute-force

  (i.e. try all the possible keys till a key that works is found)
  - Super Computer can crack a 56-bit key in 24 hours
  - It will take 2^{72} times longer to crack a 128-bit key

    (Longer than the age of the universe)

Substitution Cipher

Monoalphabetic Cipher

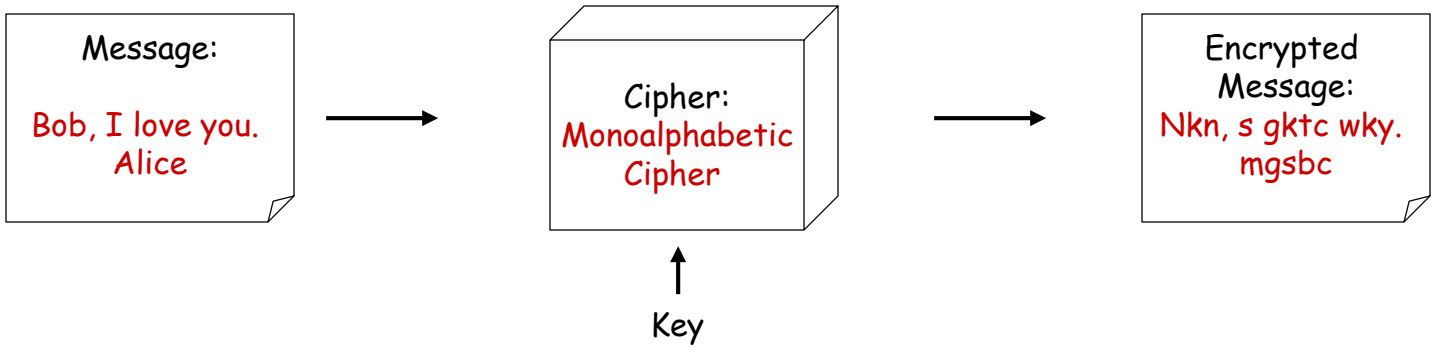
- Any letter can be substituted for any other letter
  - Each letter has to have a unique substitute

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

↓

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

- There are 26! pairing of letters ($\sim 10^{26}$)
- Brute Force approach would be too time consuming
  - Statistical Analysis would make it feasible to crack the key

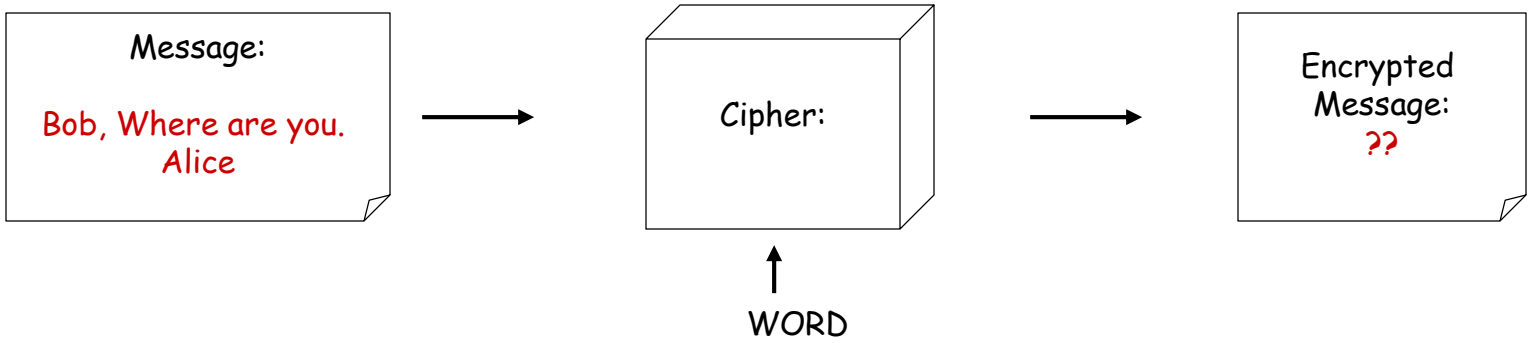


Substitution Cipher

Using a key to shift alphabet

- Obtain a key to for the algorithm and then shift the alphabets
  - For instance if the key is word we will shift all the letters by four and remove the letters w, o, r, & d from the encryption
- We have to ensure that the mapping is one-to-one
  - no single letter in plain text can map to two different letters in cipher text
  - no single letter in cipher text can map to two different letters in plain text

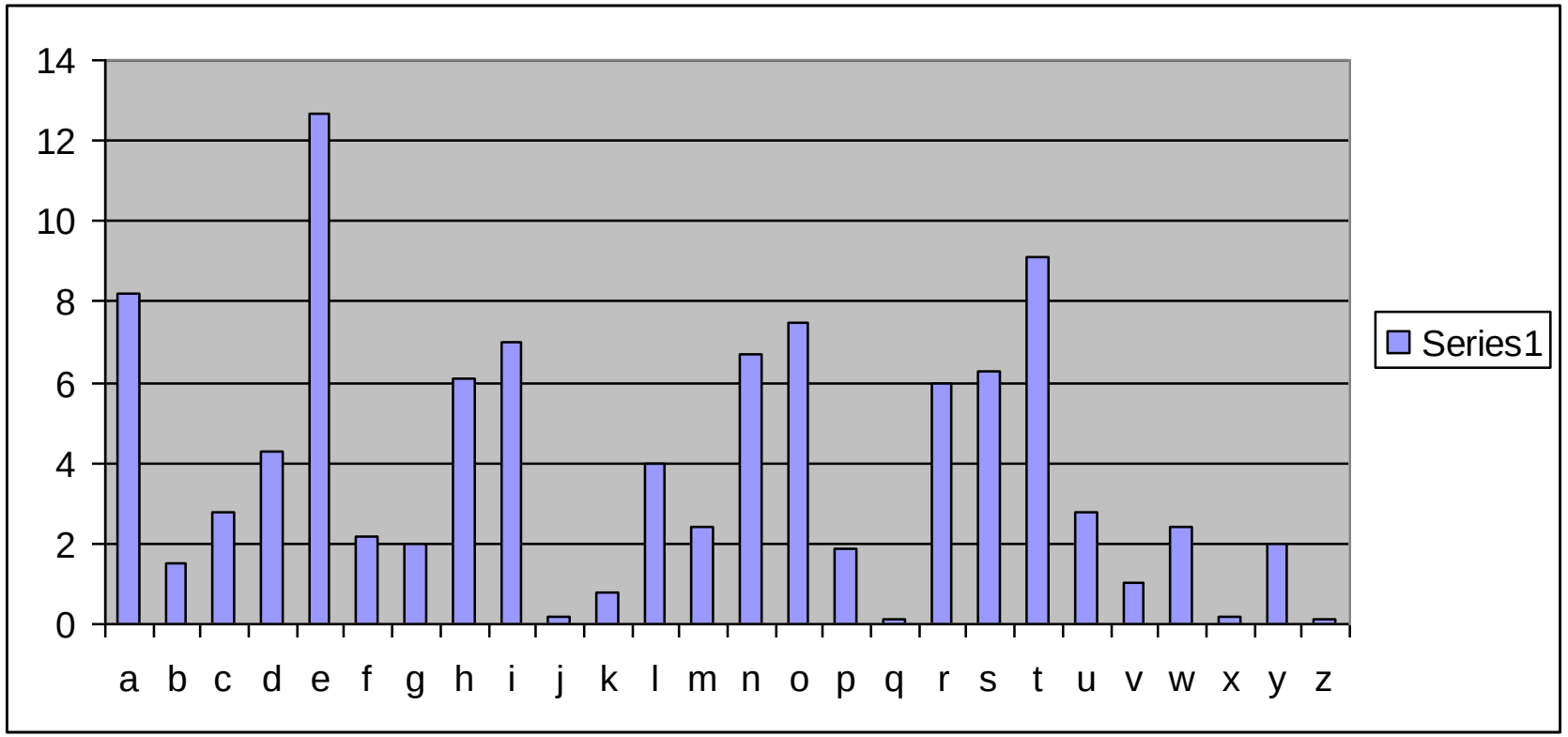
Plain Text	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
	↓
C1(k=6)	W O R D A B C E F G H I J K L M N P Q S T U V X Y Z



Character Frequencies

- In most languages letters are not equally common
  - in English **e** is by far the most common letter
- Have tables of single, double & triple letter frequencies
- Use these tables to compare with letter frequencies in ciphertext,
  - a monoalphabetic substitution does not change relative letter frequencies
  - do need a moderate amount of ciphertext (100+ letters)

Frequency of Letters in English



Permutation Cipher

Using a key to shift alphabet

- Based on altering position of plaintext characters such that:
  - $\pi^{-1}(x) = x'$ iff $\pi(x') = x$
- We have to ensure that thπe mapping is one-to-one
  - no single letter in plain text can map to two different letters in cipher text
  - no single letter in cipher text can map to two different letters in plain text

Let m = 6, and key is the following permutation

Plain Text: x	1	2	3	4	5	6
			↓			
$\pi(x)$:	3	5	1	6	4	2

Then permutation π^{-1} is as following:

Cipher Text: x	1	2	3	4	5	6
			↓			
$\pi^{-1}(x)$:	3	6	1	5	2	4

Playfair Cipher

Used in WWI and WWII

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

Key: simple

Playfair Cipher

- Use filler letter to separate repeated letters
- Encrypt two letters together
  - Same row- followed letters
    - ac--bd
  - Same column- letters under
    - qw--wi
  - Otherwise—square's corner at same row
    - ar--bq

Analysis

- Difficult using frequency analysis
  - But it still reveals the frequency information

Letter Frequency Analysis

- Single Letter
  - A,B,C,D,E,…..
- Double Letter
  - TH,HE,IN,ER,RE,ON,AN,EN,….
- Triple Letter
  - THE,AND,TIO,ATI,FOR,THA,TER,RES,…

How to Defeat Frequency Analysis?

- Use larger blocks as the basis of substitution. Rather than substituting one letter at a time, substitute 64 bits at a time, or 128 bits.
- Use different substitutions to get rid of frequency features.
  - Leads to polyalphabetical substituion ciphers

Polyalphabetic Substitution

- Use more than one substitution alphabet
- Makes cryptanalysis harder
  - since have more alphabets to guess
  - and flattens frequency distribution
    - same plaintext letter gets replaced by several ciphertext letter, depending on which alphabet is used

Transposition Methods

- Permutation of plaintext
- Example
  - Write in a square in row, then read in column order specified by the key
- Enhance: double or triple transposition
  - Can reapply the encryption on ciphertext

Transposition Cipher

Columnar Transposition

- This involves rearrangement of characters on the plain text into columns
- The following example shows how letters are transformed
  - If the letters are not exact multiples of the transposition size there may be a few short letters in the last column which can be padded with an infrequent letter such as x or z

Plain Text

```
T H I S I
S A M E S
S A G E T
O S H O W
H O W A C
O L U M N
A R T R A
N S P O S
I T I O N
W O R K S
```

Cipher Text

```
T S S O H
O A N I W
H A A S O
L R S T O
I M G H W
U T P I R
S E E O A
M R O O K
I S T W C
N A S N S
```

Vigenère Cipher

- Basically multiple Caesar ciphers
- key is multiple letters long
  - $K = k_1\ k_2\ \ldots\ k_d$
  - *i*th letter specifies *i*th alphabet to use
  - use each alphabet in turn, repeating from start after d letters in message
- Plaintext THISPROCESSCANALSOBEEXPRESSED
  Keyword CIPHERCIPHERCIPHERCIPHERCIPHE
  Ciphertext VPXZTIQKTZWTCVPSWFDMTETIGAHLH

The Vigenère Cipher

Treat letters as numbers: [A=0, B=1, C=2, …, Z=25]

Number Theory Notation: $Z_n = \{0, 1, \ldots, n-1\}$

Definition:

Given m, a positive integer, $P = C = (Z_{26})^n$, and $K = (k_1, k_2, \ldots, k_m)$ a key, we define:

Encryption:

$e_k(p_1, p_2 \ldots p_m) = (p_1+k_1, p_2+k_2 \ldots p_m+k_m) \pmod{26}$

Decryption:

$d_k(c_1, c_2 \ldots c_m) = (c_1-k_1, c_2-k_2 \ldots c_m-k_m) \pmod{26}$

Mathematically: $C_i = (P_i + k_{i \bmod m}) \bmod 26$

$P_i = (C_i - k_{i \bmod m}) \bmod 26$

Example:

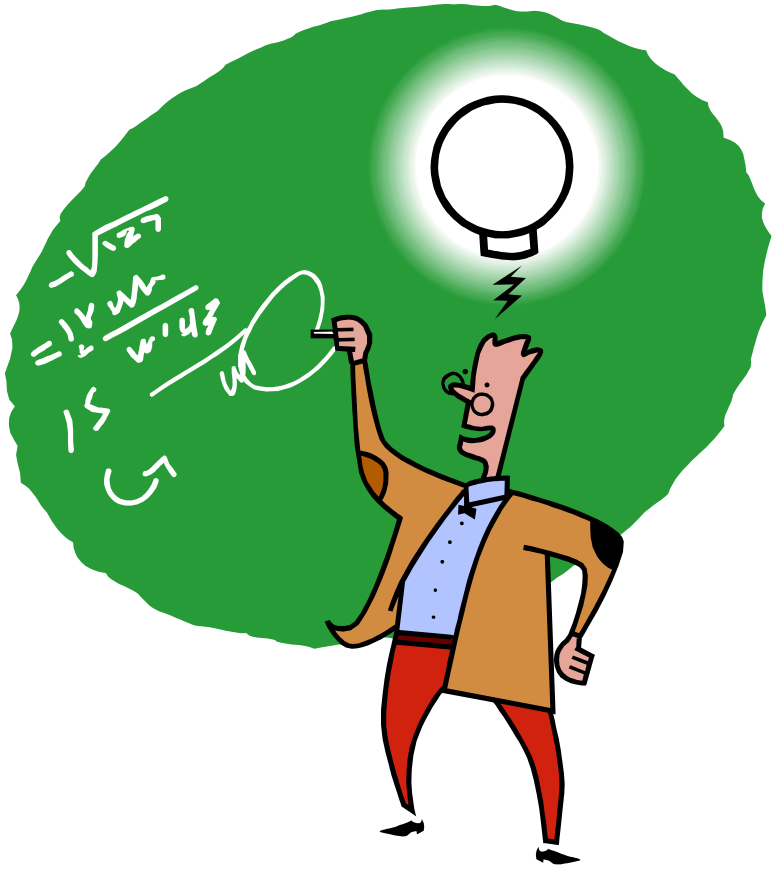
Plaintext: C R Y P T O G R A P H Y

Key: L U C K L U C K L U C K

Ciphertext: N L A Z E I I B L J J I

Vigenere Cipher: Cryptanalysis

- Somehow guess/find the length of the key.
  - Index of coincidence
- Divide the message into that many shift cipher encryptions.
  - Use frequency analysis to solve the resulting shift ciphers.

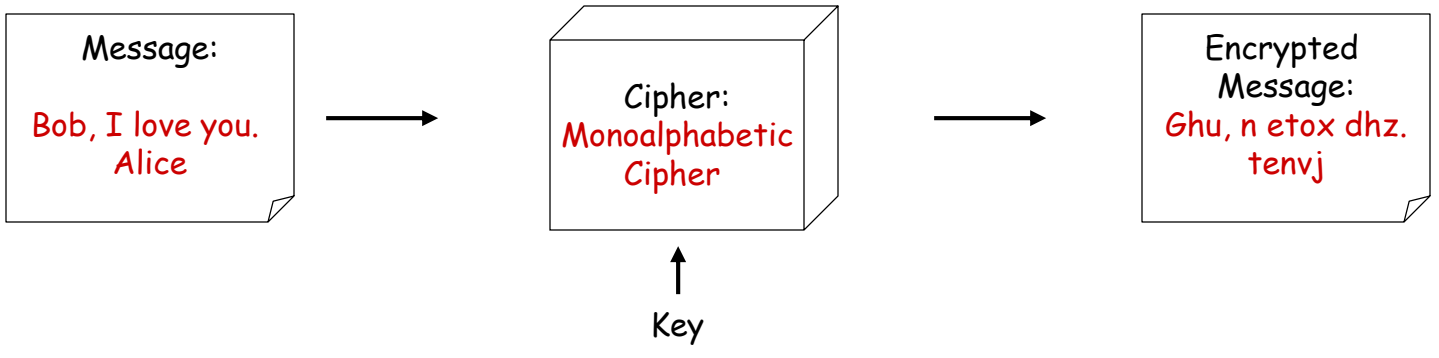


Another variant

- Uses a sequence of monoalpabetic ciphers in tandem
  - e.g. C_1, C_2, C_2, C_1, C_2

Plain Text	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
	↓
C1(k=6)	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
C2(k=20)	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S

- Example

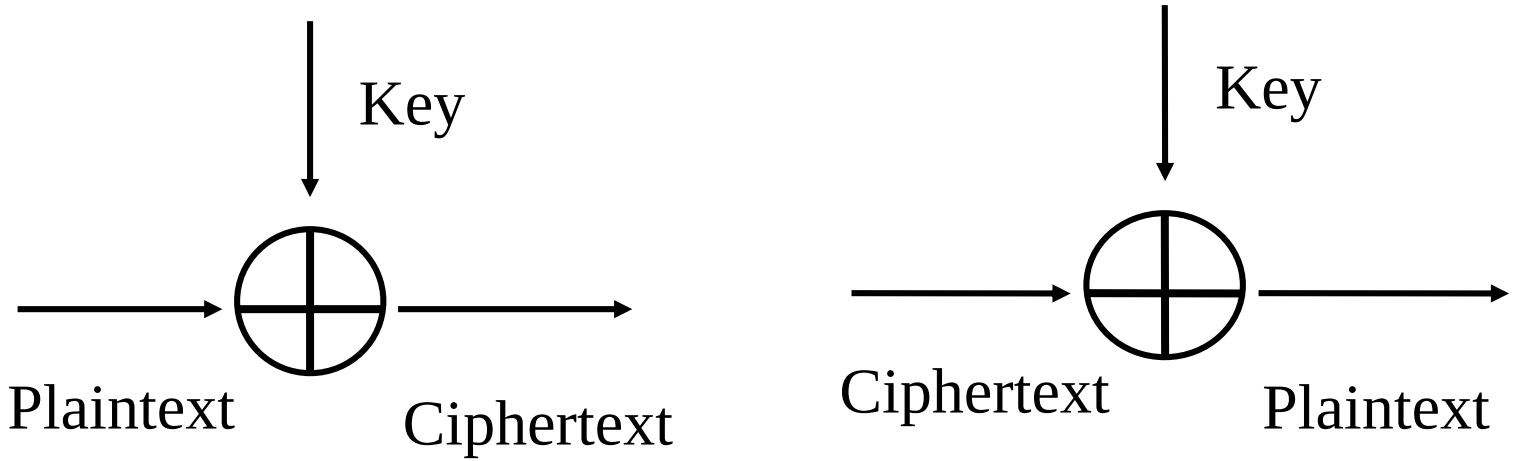


One-Time Pad

- Fix the vulnerability of the Vigenere cipher by using very long keys

- Key is a random string that is at least as long as the plaintext
- Encryption is similar to shift cipher
- Invented by Vernam in the 1920s

Stream Cipher



One-time Pad

- theoretically unbreakable (Claude Shannon)
  - the plaintext is combined with a random "*pad*" the same length as the plaintext.
- Patent by
  - Gilbert Vernam (AT&T) and Joseph Mauborgne
- Encryption
  - $C=P \oplus K$
- Decryption
  - $P=C \oplus K$
- Claude Shannon's work can be interpreted as
  - that any information-theoretically secure cipher will be effectively equivalent to the one-time pad algorithm. Hence one-time pads offer the best possible mathematical security of any encryption scheme, anywhere and anytime.

One-time pad--cont

- Drawbacks
  - it requires secure exchange of the one-time pad material, which must be as long as the message
  - pad disposed of correctly and never reused
- In practice
  - Generate a large number of random bits,
  - Exchange the key material securely between the users before sending a one-time enciphered message,
  - Keep both copies of the key material for each message securely until they are used, and
  - Securely dispose of the key material after use, thereby ensuring the key material is never reused.

One-Time Pad

Let $Z_m = \{0,1,\ldots,m-1\}$ be the alphabet.

Plaintext space = Ciphtertext space = Key space = $(Z_m)^n$

The key is chosen uniformly randomly

Plaintext $X = (x_1\ x_2\ \ldots\ x_n)$

Key $K = (k_1\ k_2\ \ldots\ k_n)$

Ciphertext $Y = (y_1\ y_2\ \ldots\ y_n)$

$e_k(X) = (x_1+k_1\ \ x_2+k_2\ \ldots\ x_n+k_n) \bmod m$

$d_k(Y) = (y_1-k_1\ \ y_2-k_2\ \ldots\ \ y_n-k_n) \bmod m$

The Binary Version of One-Time Pad

Plaintext space = Ciphtertext space =

Keyspace = $\{0,1\}^n$

Key is chosen randomly

For example:

- Plaintext is 11011011
- Key is 01101001
- Then ciphertext is 10110010

Bit Operators

- Bit AND

  $0 \wedge 0 = 0$ $0 \wedge 1 = 0$ $1 \wedge 0 = 0$ $1 \wedge 1 = 1$

- Bit OR

  $0 \vee 0 = 0$ $0 \vee 1 = 1$ $1 \vee 0 = 1$ $1 \vee 1 = 1$

- Addition mod 2 (also known as Bit XOR)

  $0 \oplus 0 = 0$ $0 \oplus 1 = 1$ $1 \oplus 0 = 1$ $1 \oplus 1 = 0$

- Can we use operators other than Bit XOR for binary version of One-Time Pad?

Key Randomness in One-Time Pad

- One-Time Pad uses a very long key, what if the key is not chosen randomly, instead, texts from, e.g., a book are used as keys.
  - this is not One-Time Pad anymore
  - this can be broken
  - How?
- Corrolary: The key in One-Time Pad should never be reused.
  - If it is reused, it is Two-Time Pad, and is insecure!
  - Why?

Usage of One-Time Pad

- To use one-time pad, one must have keys as long as the messages.
- To send messages totaling certain size, sender and receiver must agree on a shared secret key of that size.
  - typically by sending the key over a secure channel
- Key agreement is difficult to do in practice.
- Why is OTP still useful, even though difficult to use?

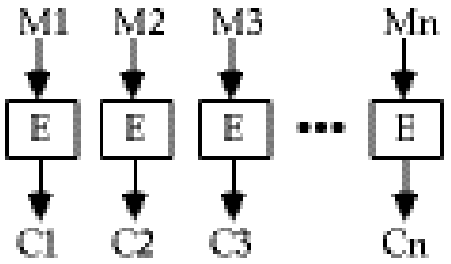
Usage of One-Time Pad

- The channel for distributing keys may exist at a different time from when one has messages to send.

- The channel for distributing keys may have the property that keys can be leaked, but such leakage will be detected

Block Ciphers

- The message is broken into blocks,
  - Each of which is then encrypted
  - (Like a substitution on very big characters - 64-bits or more)



Substitution and Permutation

- In his 1949 paper Shannon also introduced the idea of substitution-permutation (S-P) networks, which now form the basis of modern block ciphers
  - An S-P network is the modern form of a substitution-transposition product cipher
  - S-P networks are based on the two primitive cryptographic operations we have seen before

Substitution

- A binary word is replaced by some other binary word
- The whole substitution function forms the key
- If use n bit words,
  - The key space is 2^n!
- Can also think of this as a large lookup table, with n address lines (hence 2^n addresses), each n bits wide being the output value
- Will call them **s-boxes**

Permutation

- A binary word has its bits reordered (permuted)
- The re-ordering forms the key
- If use n bit words,
  - The key space is n! (Less secure than substitution)
- This is equivalent to a wire-crossing in practice
  - (Though is much harder to do in software)
- Will call these **p-boxes**

Substitution-permutation Network

- Shannon combined these two primitives
- He called these **mixing transformations**
- A special form of product ciphers where
  - **S-boxes**
    - Provide **confusion** of input bits
  - **P-boxes**
    - Provide **diffusion** across s-box inputs

Confusion and Diffusion

- **Confusion**
  - A technique that seeks to make the relationship between the statistics of the ciphertext and the value of the encryption keys as complex as possible. Cipher uses key and plaintext.
- **Diffusion**
  - A technique that seeks to obscure the statistical structure of the plaintext by spreading out the influence of each individual plaintext digit over many ciphertext digits.

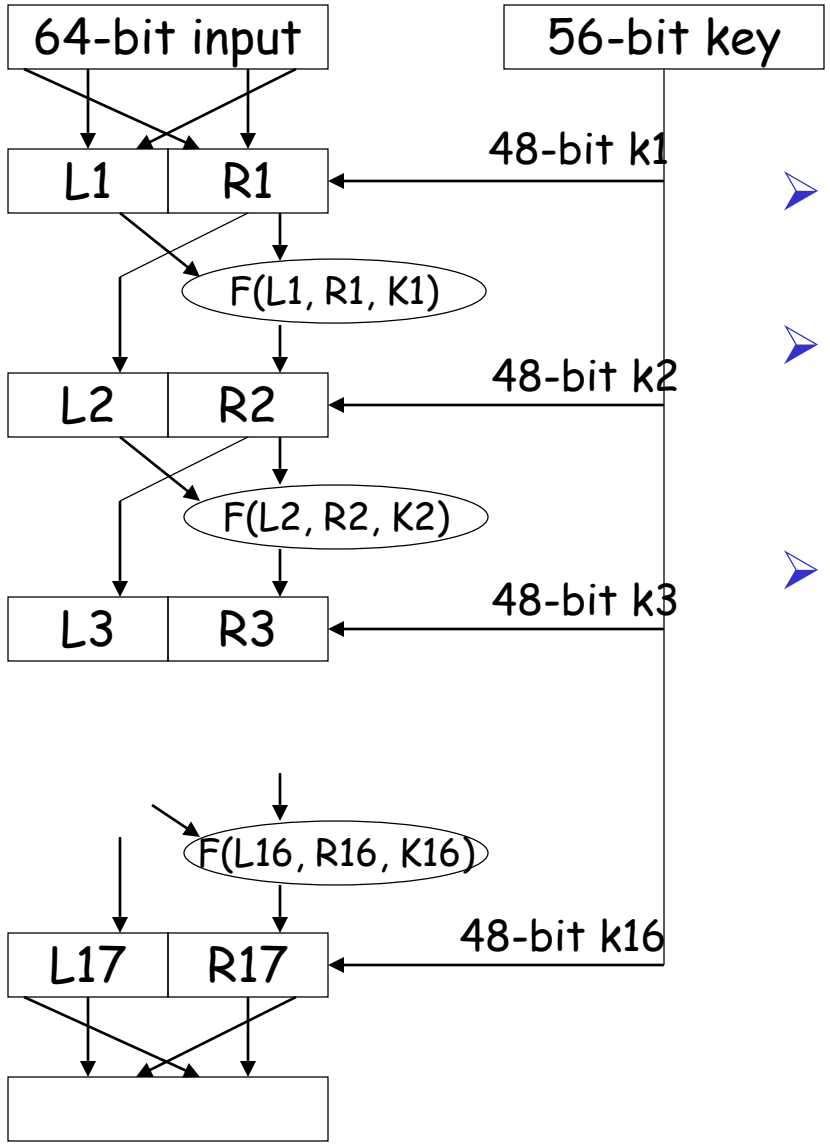
Desired Effect

- Avalanche effect
  - A characteristic of an encryption algorithm in which a small change in the plaintext gives rise to a large change in the ciphertext
  - Best: changing *one* input bit results in changes of approx *half* the output bits
- Completeness effect
  - where each output bit is a complex function of *all* the input bits

Practical Substitution-permutation Networks

- In practice we need to be able to decrypt messages, as well as to encrypt them, hence either:
  - Have to define inverses for each of our S & P-boxes, but this doubles the code/hardware needed, or
  - Define a structure that is easy to reverse, so can use basically the same code or hardware for both encryption and decryption

Data Encryption Standard (DES) Basics



- DES run in reverse to decrypt
- Cracking DES
  - 1997: 140 days
  - 1999: 14 hours
- TripleDES uses DES 3 times in tandem
  - Output from 1 DES is input to next DES

Ciphers

Shannon's Characteristics of "Good" Ciphers

- The amount of secrecy needed should determine the amount of labor appropriate for the encryption and decryption.
- The set of keys and the enciphering algorithm should be free from complexity.
- The implementation of the process should be as simple as possible.
- Errors in ciphering should not propagate and cause corruption of further information in the message.
- The size of the enciphered text should be no larger than the text of the original message.

Encryption Systems

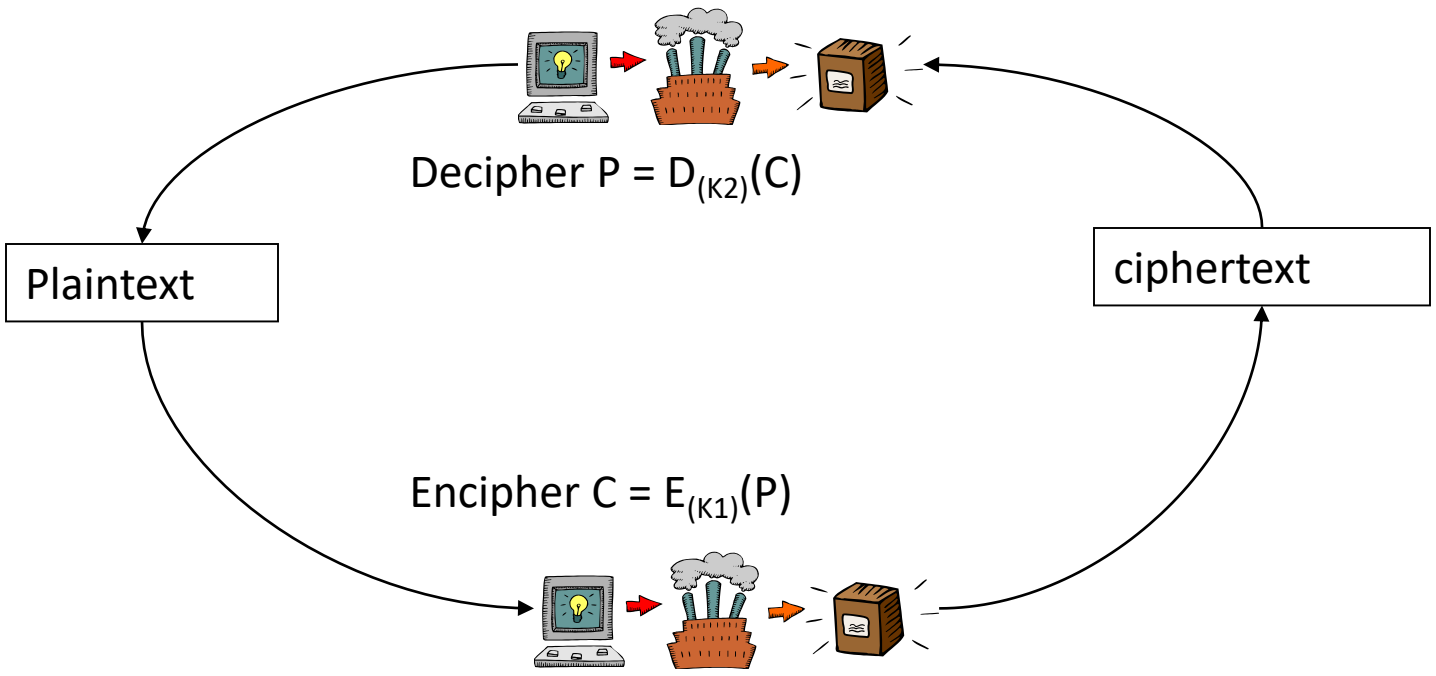
Properties of Trustworthy Systems

- It is based on sound mathematics.
  - Good cryptographic algorithms are are derived from solid principles.
- It has been analyzed by competent experts and found to be sound.
  - Since it is hard for the writer to envisage all possible attacks on the algorithm
- It has stood the "test of time."
  - Over time people continue to review both mathematical foundations of an algorithm and the way it builds upon those foundations.
  - The flaws in most algorithms are discovered soon after their release.

Key Management

- Using secret channel
- Encrypt the key
- Third trusted party
- The sender and the receiver generate key
  - The key must be same
  - We will talk more about how we can generate keys for two parties who are “unknown” of each other before, and want secure communication

Next: Asymmetric Key Cryptography



K1, K2: from keyspace