Security and Applications

Grading

- Grading
  - Quiz/Assignments/Homeworks: 15%
  - Minors (closed book): 15% + 15%
  - Project work and report 20%
    - Select your own topic
    - 10 to 15 pages report
  - Final exam (closed book): 30%
  - Class participation: 5%
- Policy
  - Do it yourself
  - Innovative outlook

Topics

- Cryptography
- Security in Digital enterprises
- Blockchain/Cloud security

Attacks, Services and Mechanisms

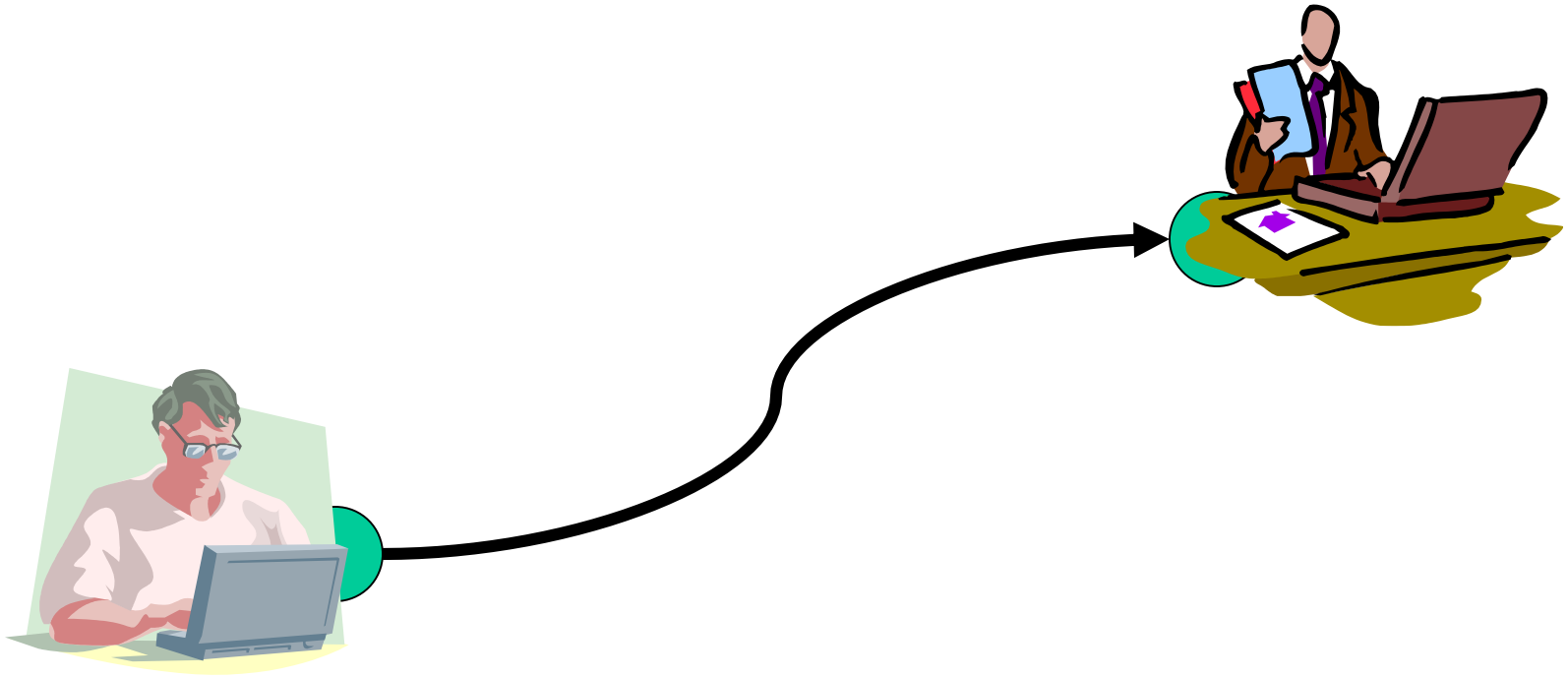
- Security Attacks
  - Action compromises the information security
- Security Services
  - Security of data processing and transferring
- Security mechanism
  - Detect, prevent and recover from a security attack

How security of systems can be compromised?

Attacks

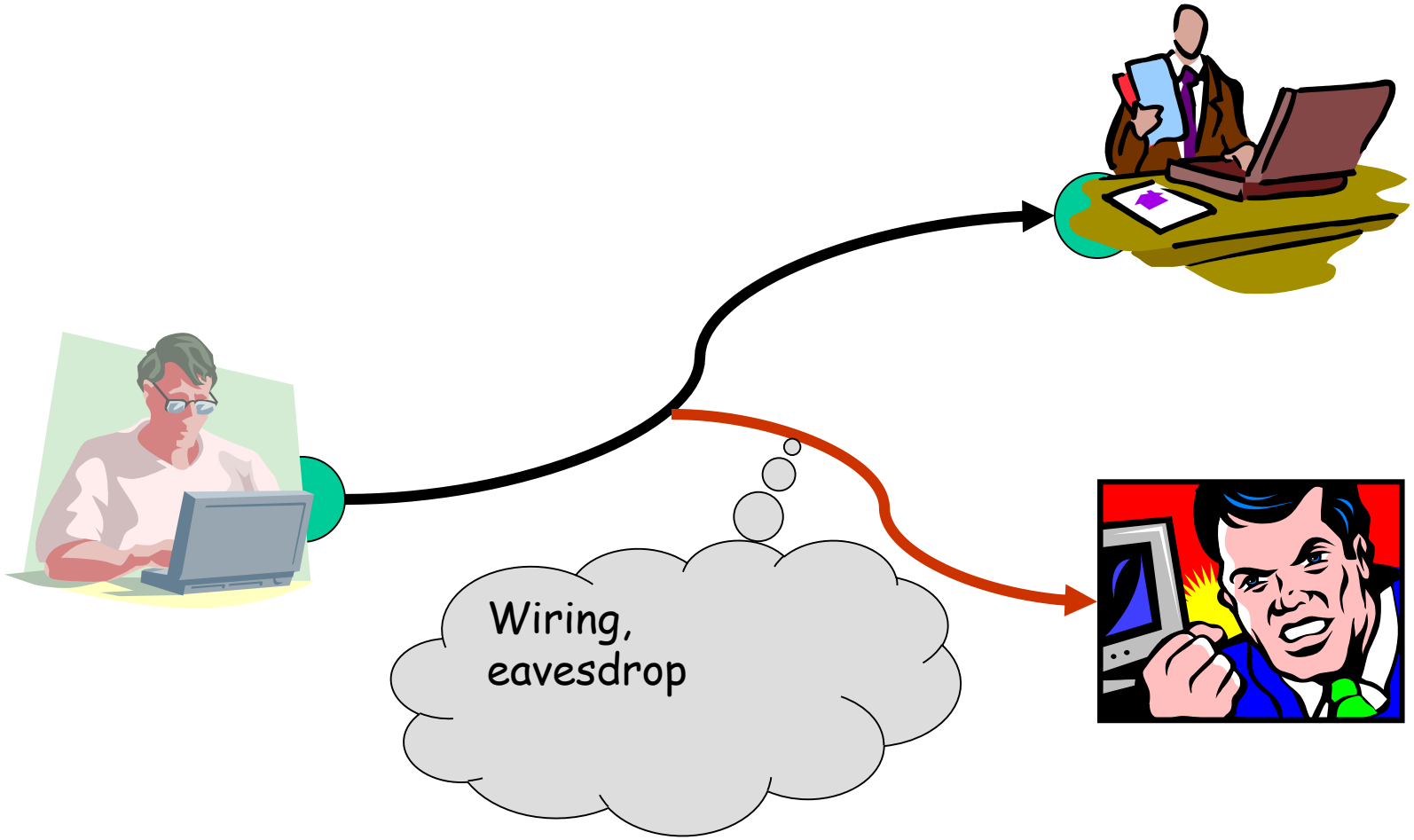
- Malware
- Cybersquatting
- Phishing
- Cyber vandalism
- Masquerading or spoofing
- Denial of Service

Information Transferring

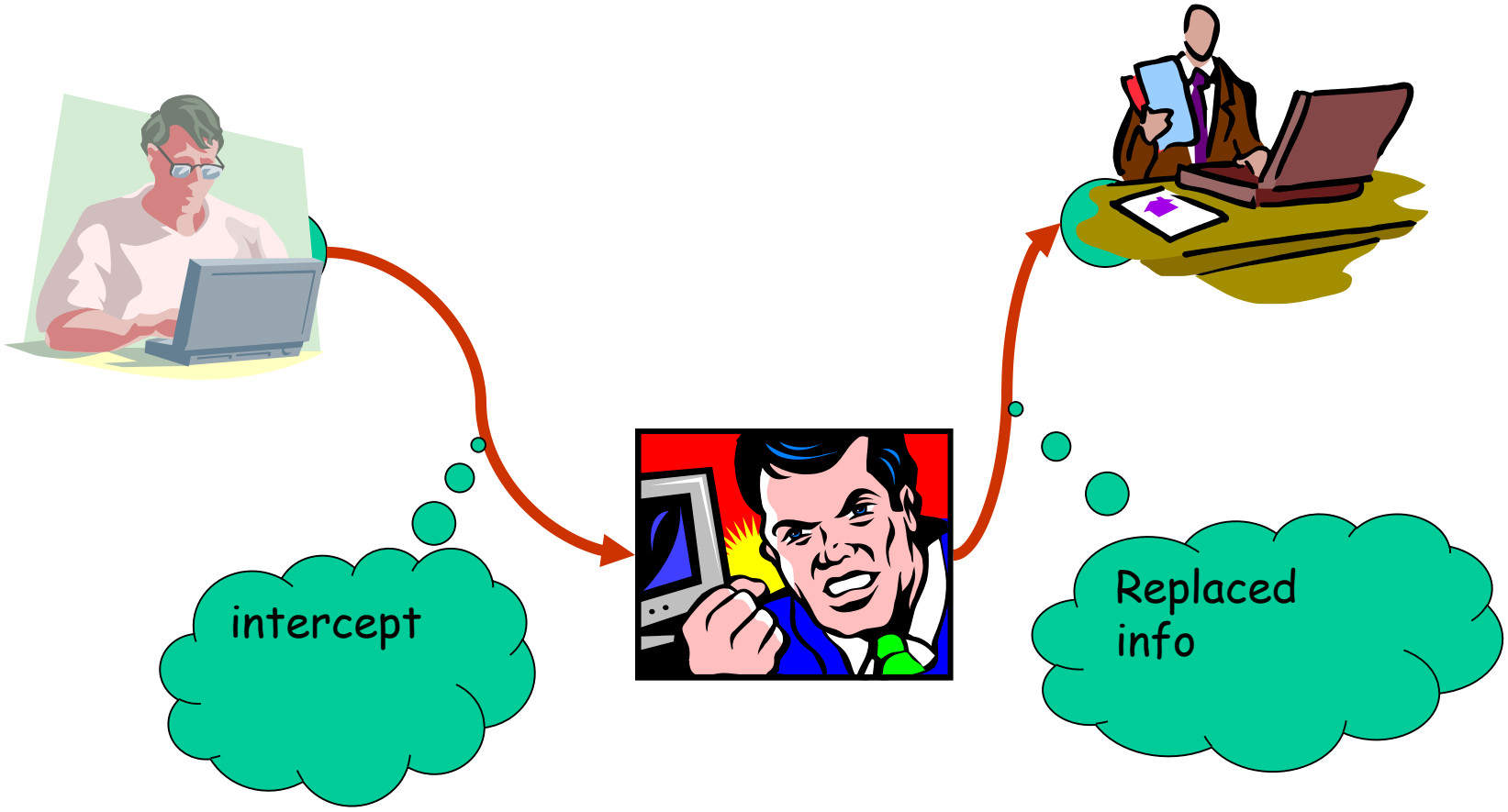


How an adversary can compromise communication

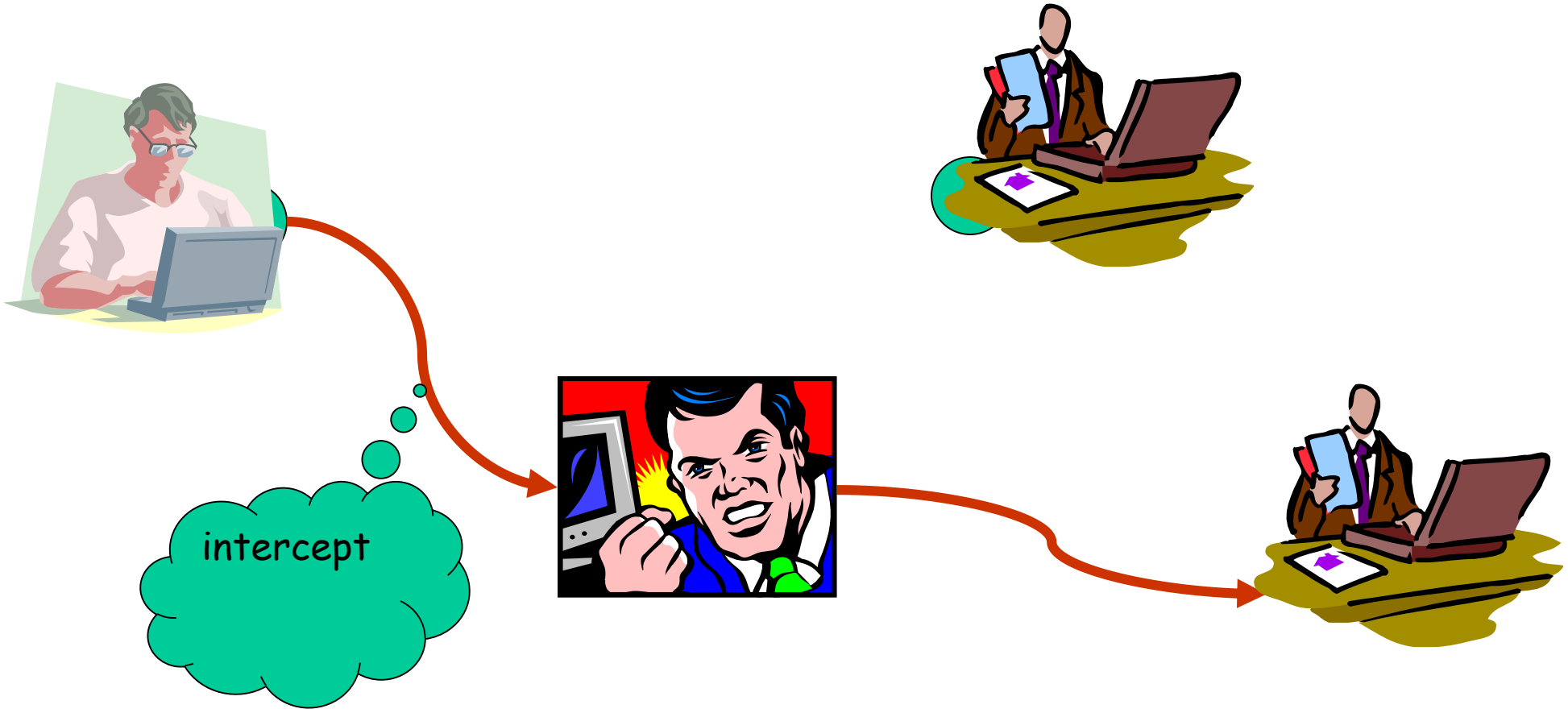
Attack: Interception



Attack: Modification



Attack: change of recipient

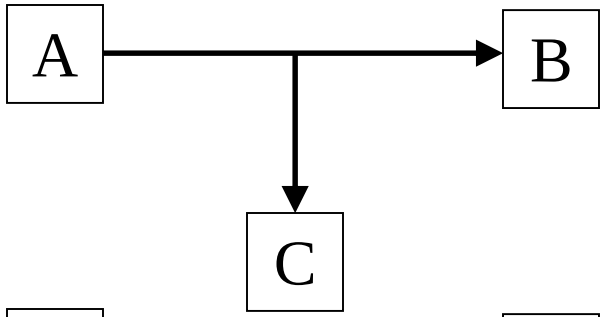


Attack: Fabrication

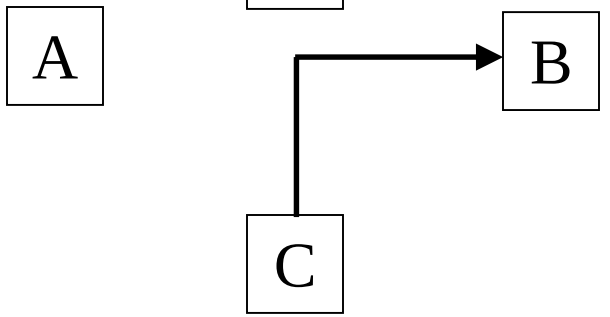
Also called impersonation

Information Transfer: Security Services

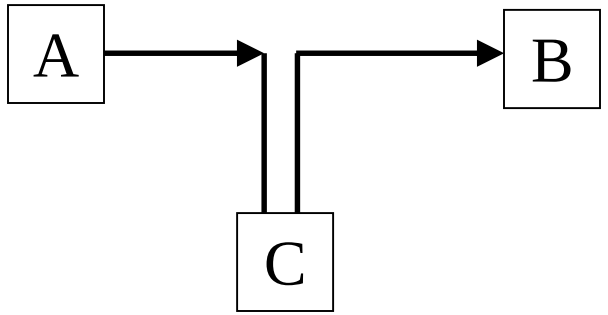
Confidentiality



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

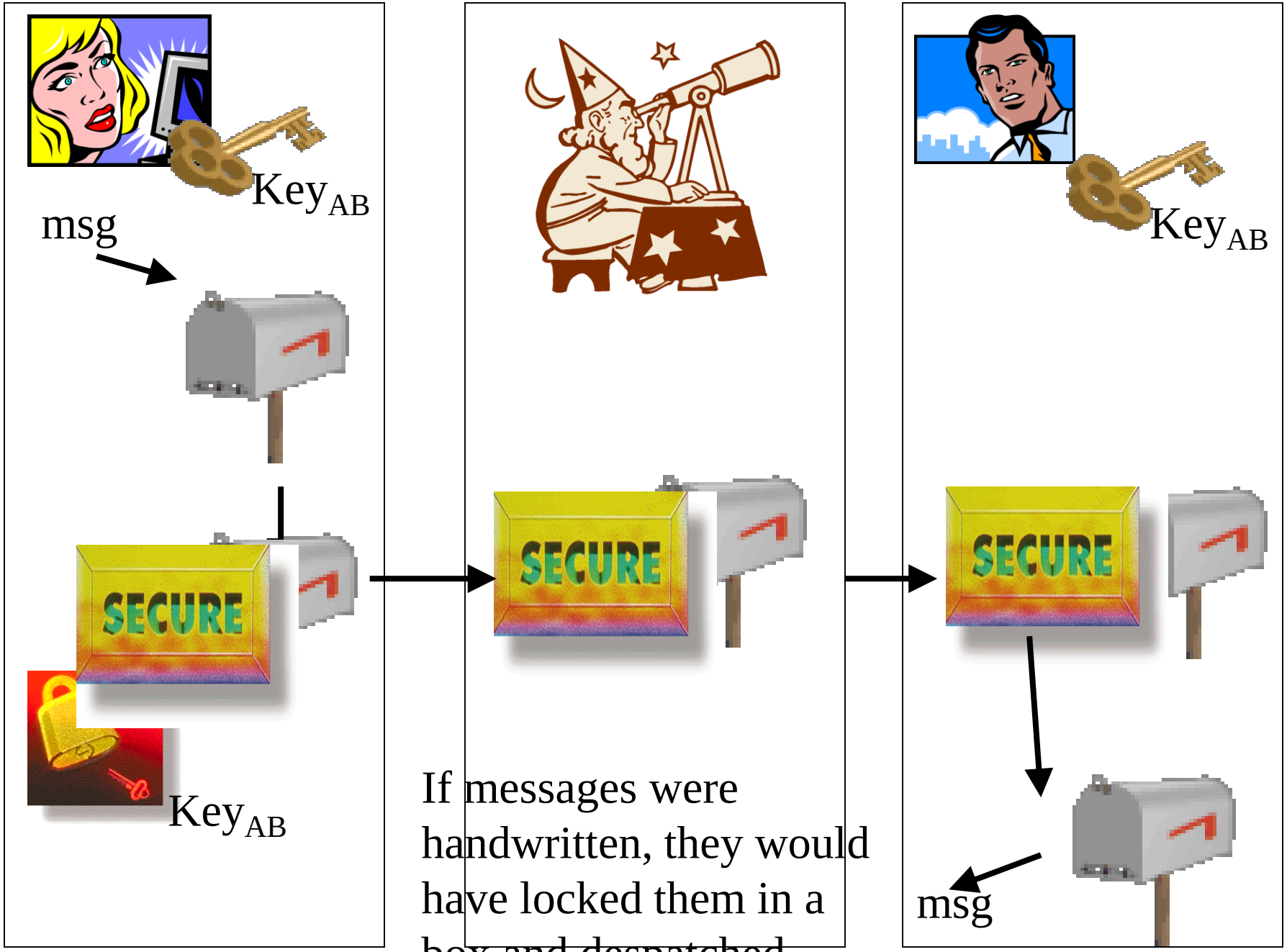
Cryptography

- **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

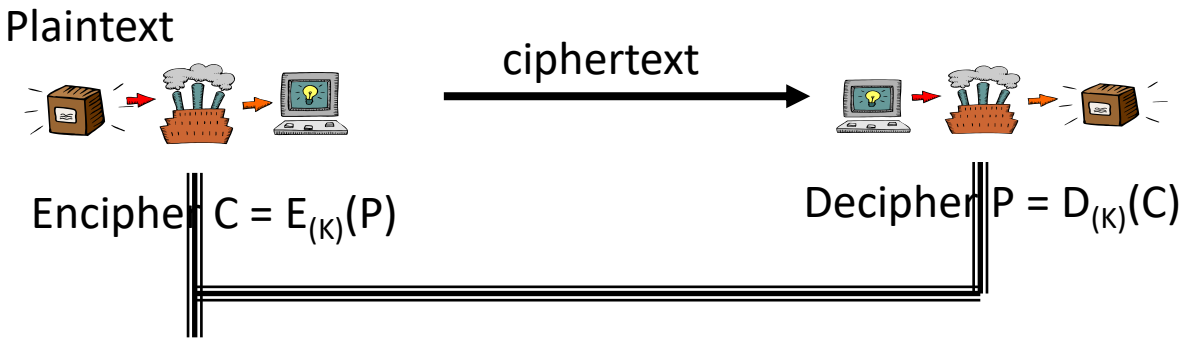
- Cost of breaking cipher exceeds the value of information.
- The time required is very high (> age of info or universe)

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

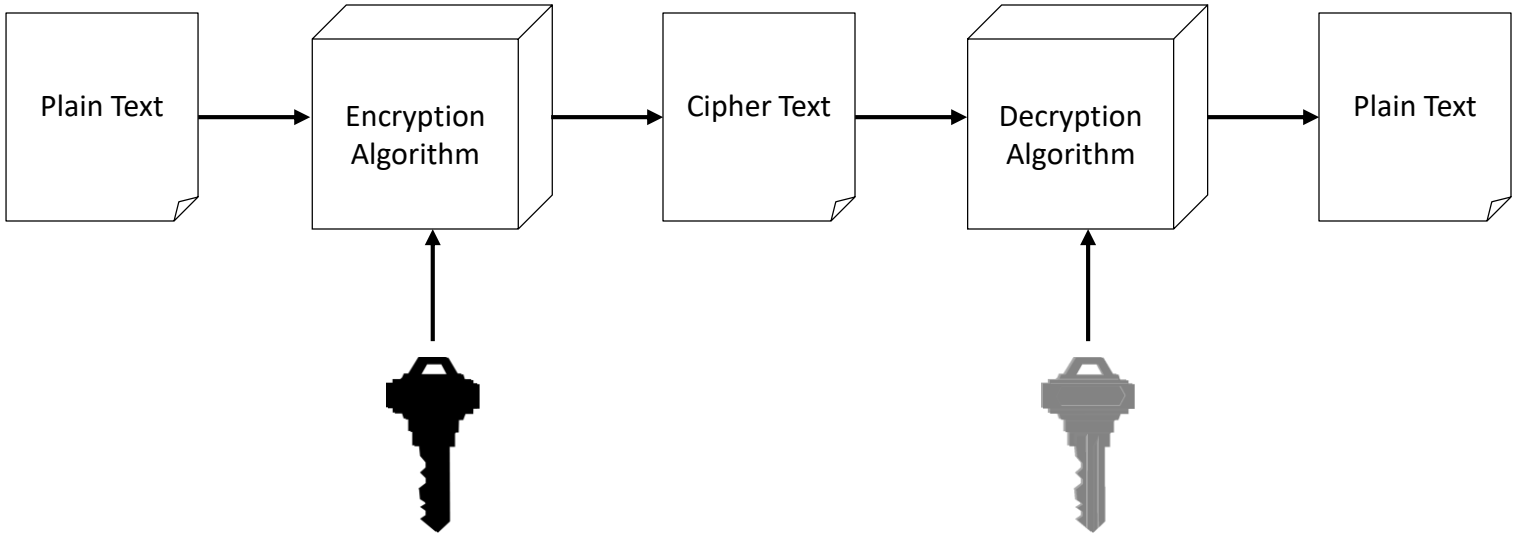
Ingredients of Cryptographic System

- **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

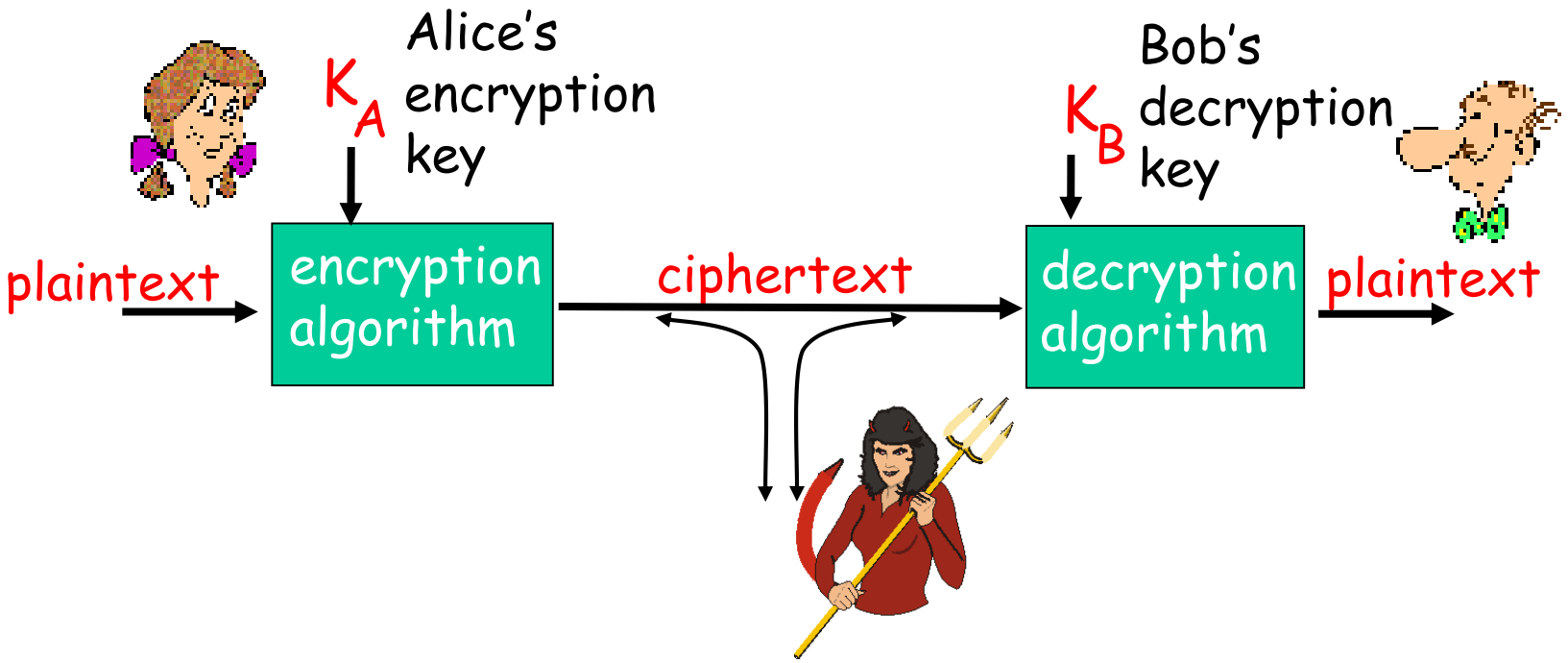
Cipher

- 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

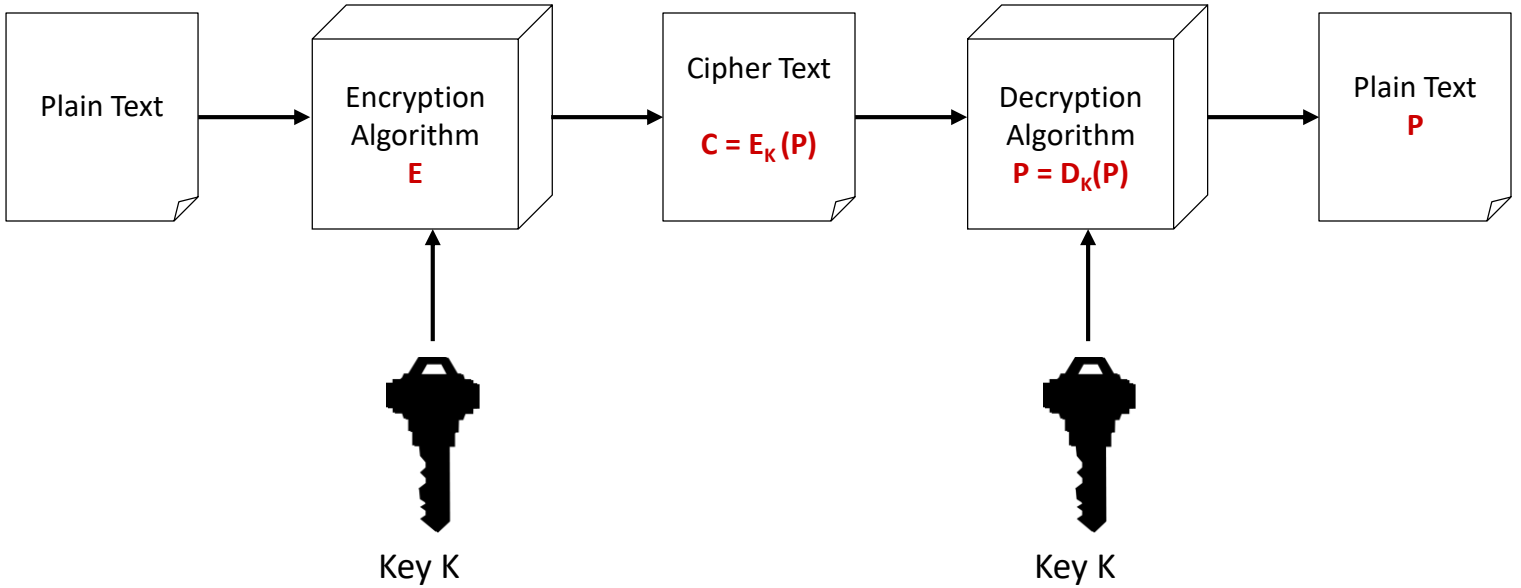
- *cipher*
  - an algorithm for encryption and decryption. The exact operation of ciphers is normally controlled by a key — some secret piece of information that customizes how the ciphertext is produced
- *Protocols*
  - specify the details of how ciphers (and other cryptographic primitives) are to 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

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

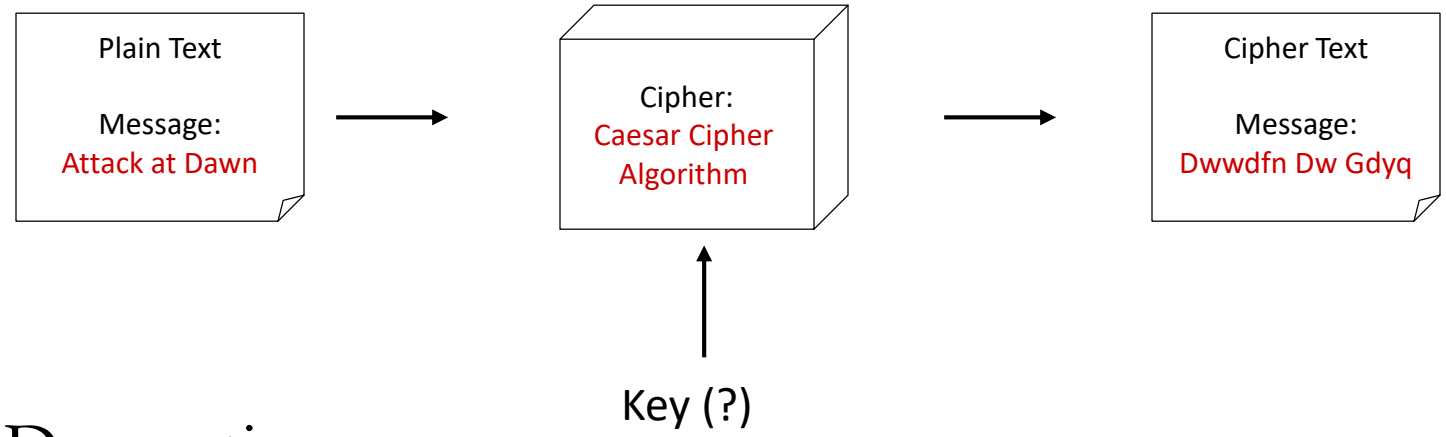
Let us try to encrypt the message

–Attack at Dawn

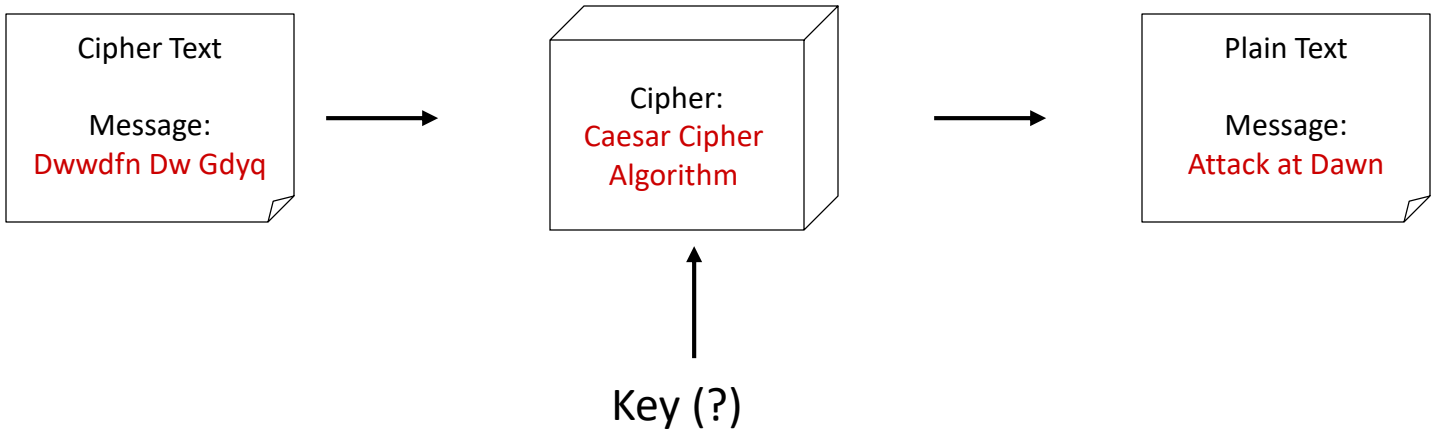
Substitution Ciphers

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

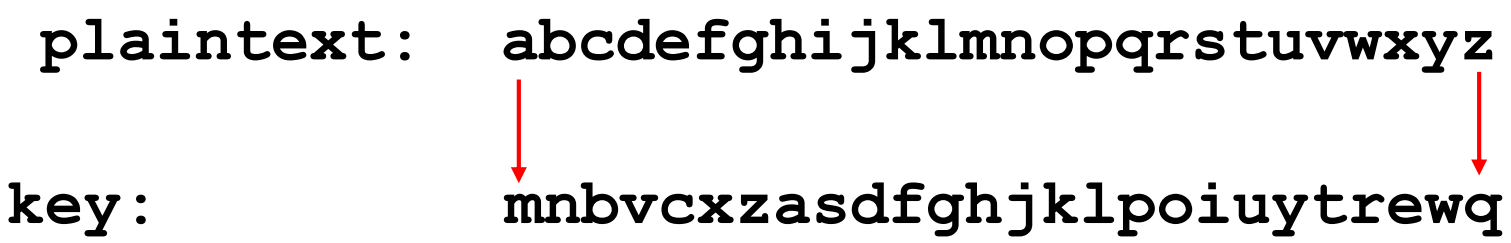
Q: How hard to break this simple cipher?:

- brute force (how hard?)
- other?

Symmetric key cryptography

substitution cipher: substituting one thing for another

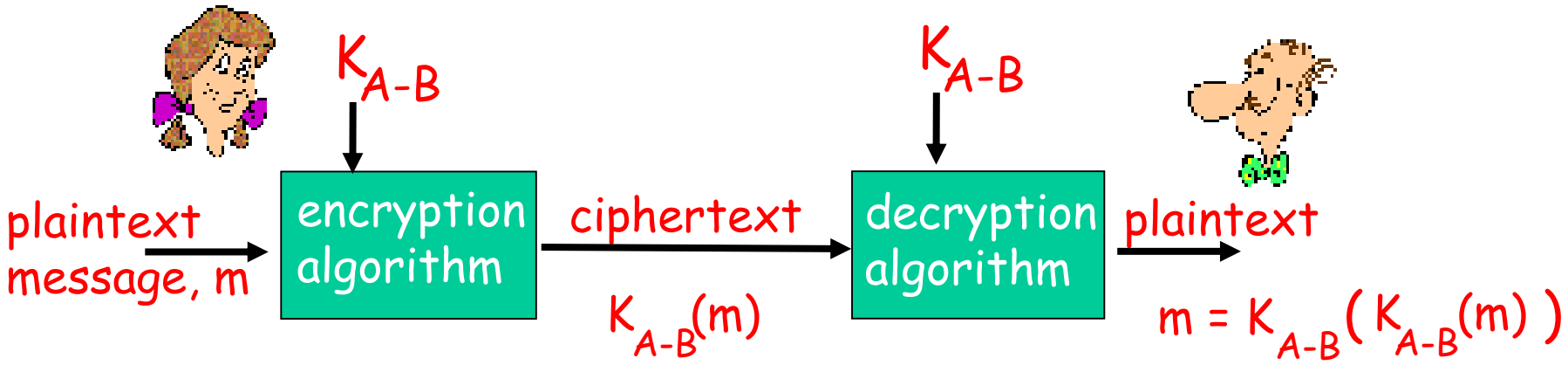
- monoalphabetic cipher: substitute one letter for another



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

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.

Affine 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 Affine 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