COMP412

Computer Security

Chapter 1
Introduction

Dr. Xiaochen Yuan
2021/2022

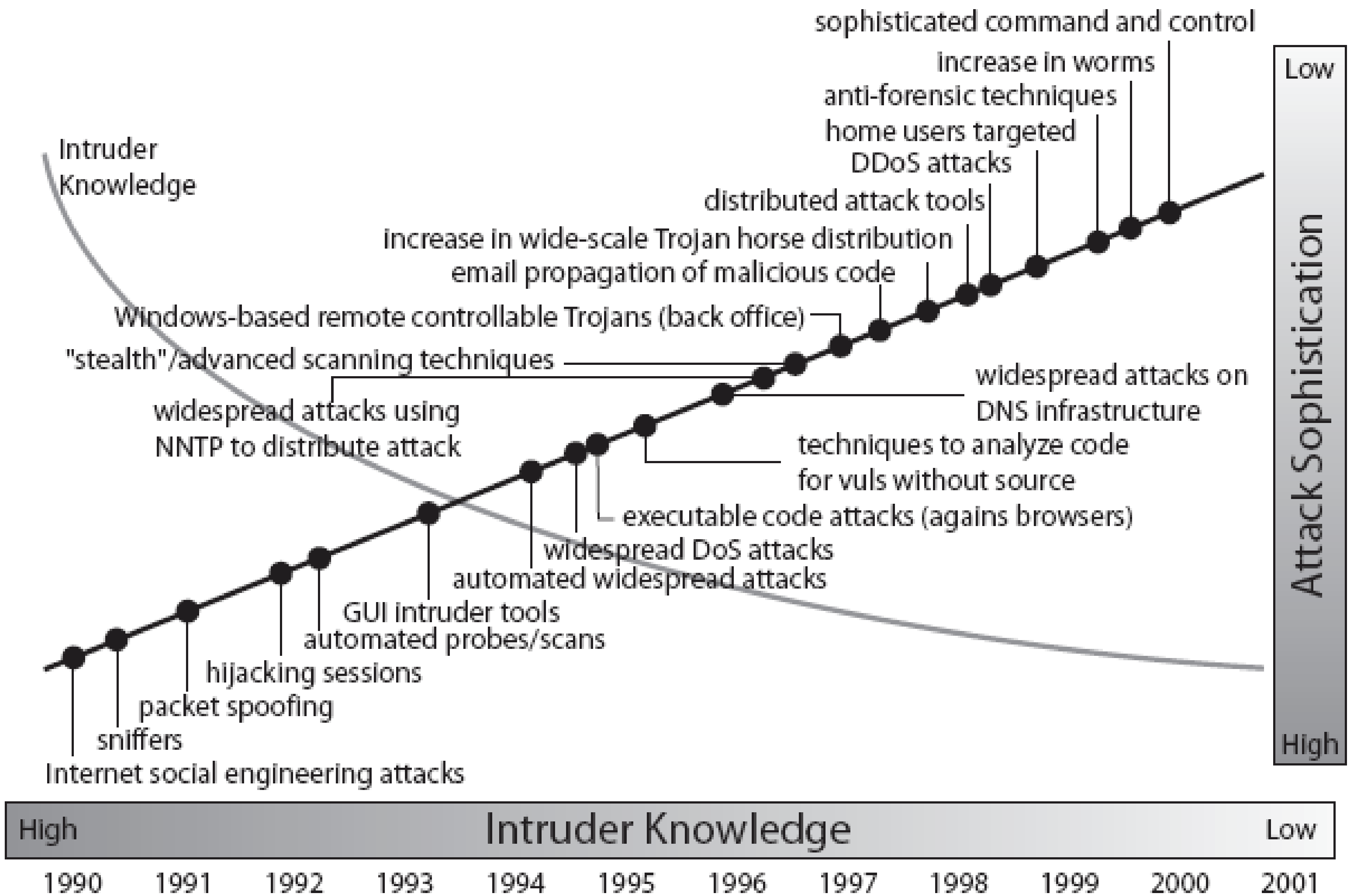
Contents

- Why Computer Security?
- Definition and Objectives
- The OSI Security Architecture
- Security Models
- Some Cryptography Terms
- Symmetric Cipher Model
- Classical Ciphers
  - Substitution ciphers
  - Transposition ciphers

Why Computer Security?

- Information is a strategic resources
  - Stored and processed within a computer
  - Transferred between computers
- Situations that you need security
  - Capture sensitive information and read by unauthorized party
  - Intercept a message, alter the content and then forward it to receiver
  - Construct a malicious message and send to receiver
  - Delay a message delivered to the receiver
  - Deny what you have done

Security Trends



Source: CERT

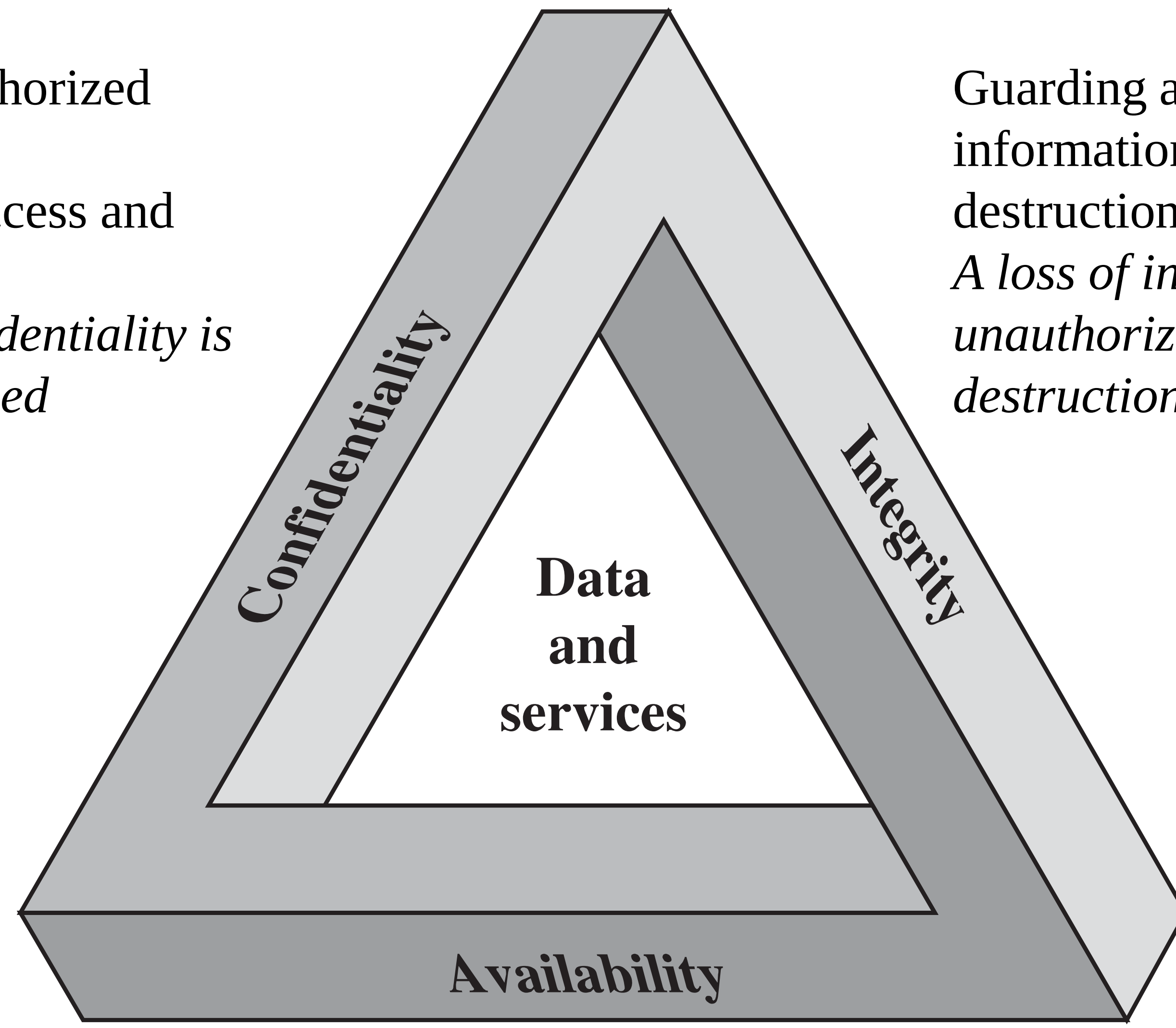
Definition of Computer Security

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the *integrity*, *availability*, and *confidentiality* of information system resources (includes hardware, software, firmware, information/ data, and telecommunications).

Objectives of Computer Security

CIA Triad

Preserving authorized restrictions on information access and disclosure.
A loss of confidentiality is the unauthorized disclosure of information.



Guarding against improper information modification or destruction.
A loss of integrity is the unauthorized modification or destruction of information.

Ensuring timely and reliable access to and use of information.
A loss of availability is the disruption of access to or use of information or an information system.

Objectives of Computer Security

- Confidentiality
  - Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  - Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- Integrity
  - Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
  - System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- Availability
  - Assures that systems work promptly and service is not denied to authorized users.

Additional Concepts to Computer Security

- Authenticity
  - The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
  - This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

- Accountability
  - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
  - Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party.
  - Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

The OSI Security Architecture

- To assess the security needs and evaluate various security products, we need a systematic way of defining requirements for security and characterizing the approaches to meet security requirements.
- Three aspects of information security will be considered.

Mechanisms	→	Services	⇄	Attacks
Public key algorithms Message digest Signatures		Authentication		Claims didn't send Impersonate someone

Security Attacks

- Any action that compromises the security of information owned by an organization
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- There are wide range of attacks and we focuses on generic types of attacks - password cracking, etc.
- Note: threat & attack are almost same

Attack and Threat

- Threat
  - *A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.*
  - *That is, a threat is a possible danger that might exploit a vulnerability.*
- Attack
  - *An assault on system security that derives from an intelligent threat;*
  - *that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.*

Passive Vs Active Attacks

- **Passive attacks**
  - Make use of information, but not affect system resources, e.g.

  a) Release of message contents

  b) Traffic analysis

  Relatively hard to detect, but easier to prevent

- **Active attacks**
  - Alter system resources or operation, e.g.

  a) Masquerade

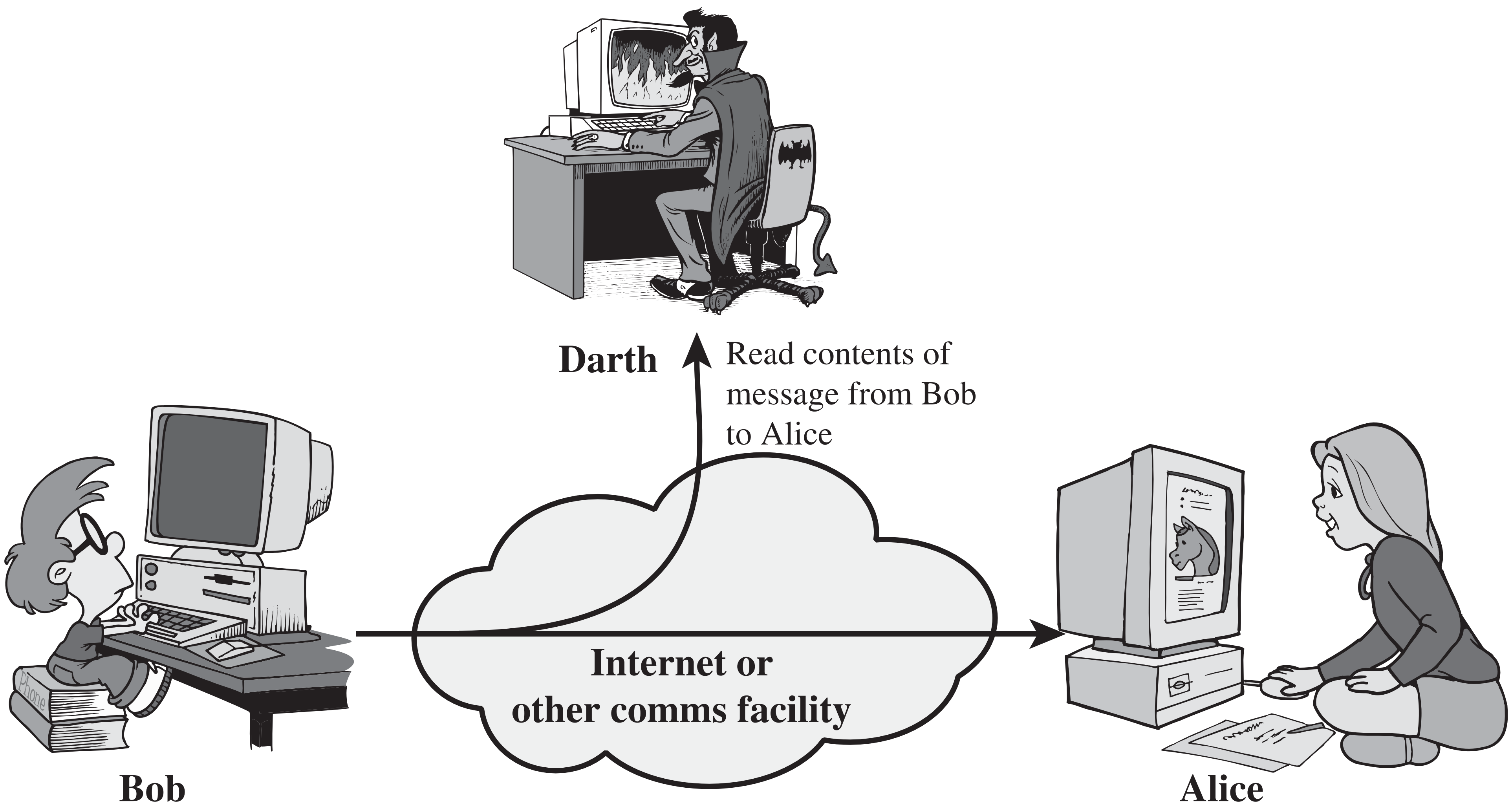
  b) Replay

  c) Modification of messages

  d) Denial of services

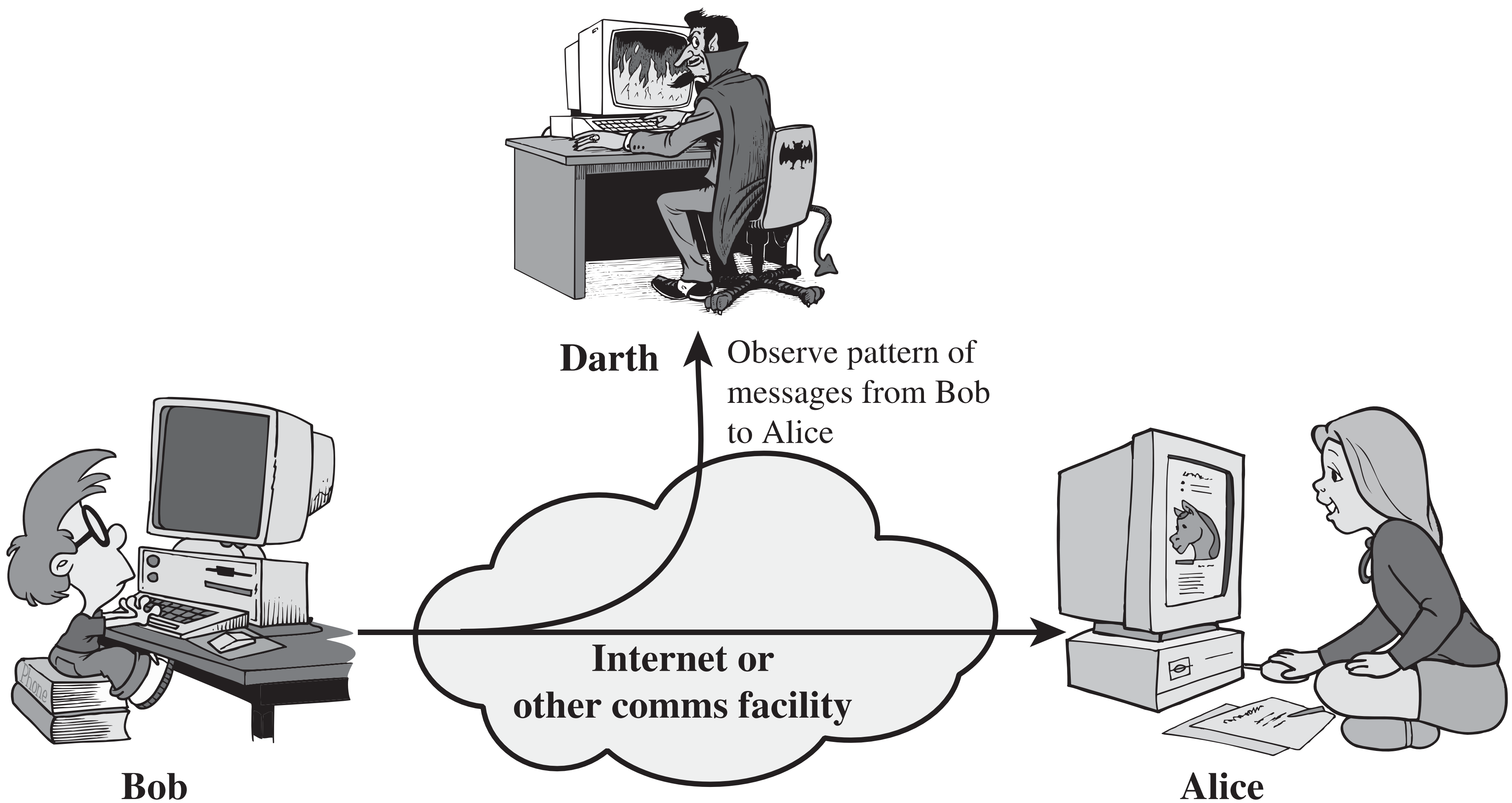
  Relatively ***hard to prevent, but easier to detect***

Passive Attacks (a)



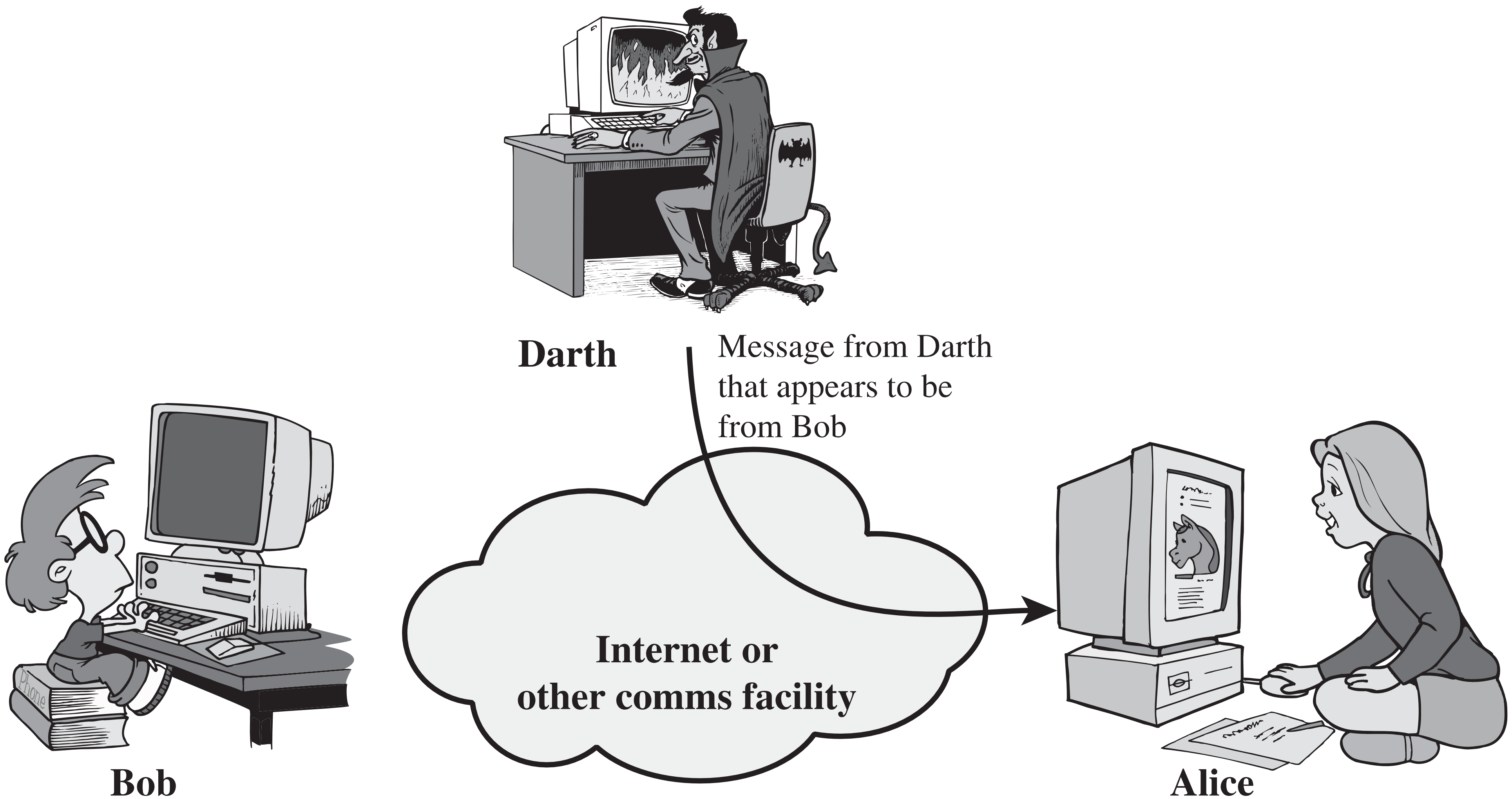
(a) Release of message contents

Passive Attacks (b)



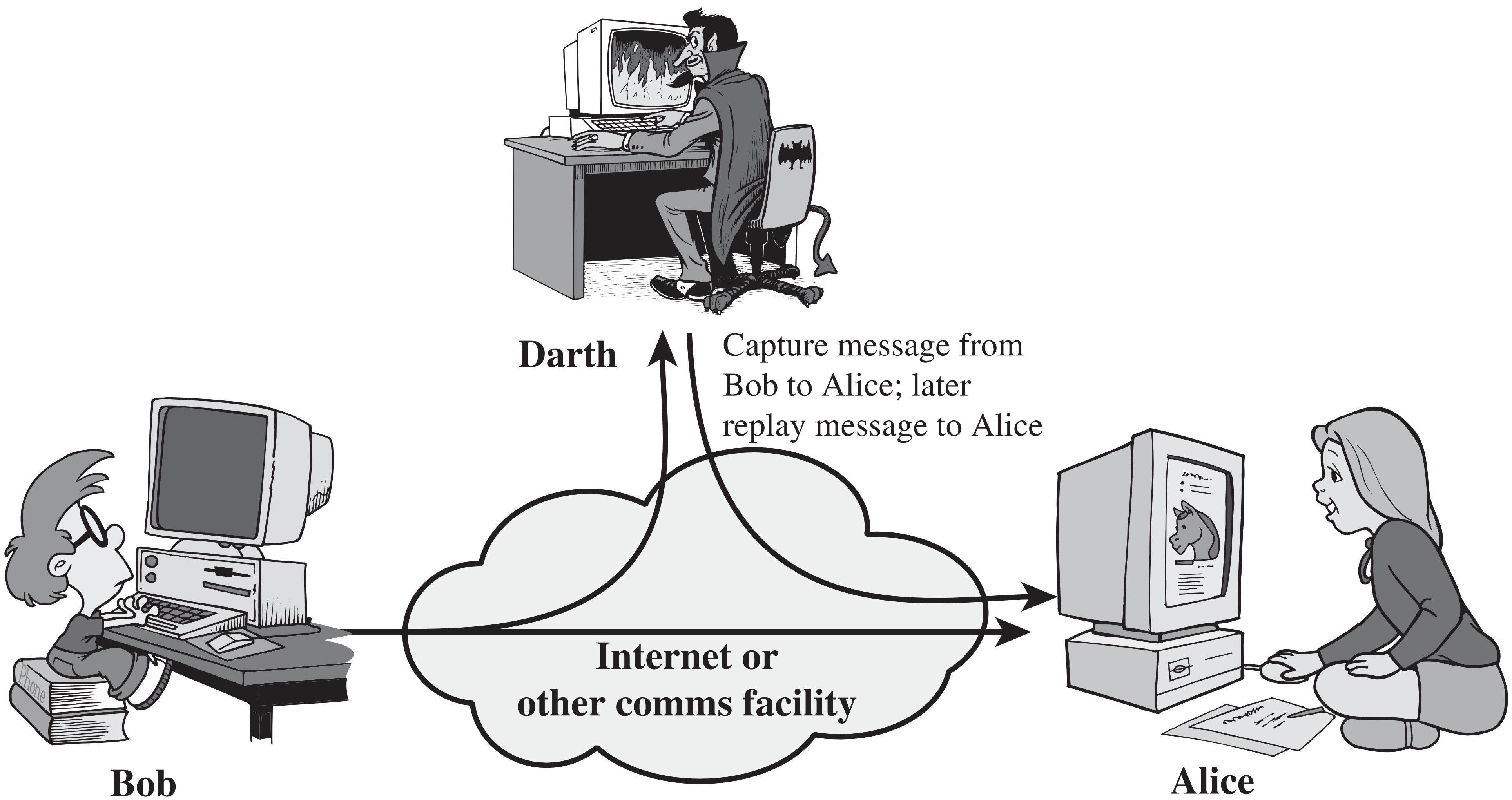
(b) Traffic analysis

Active Attacks (a)



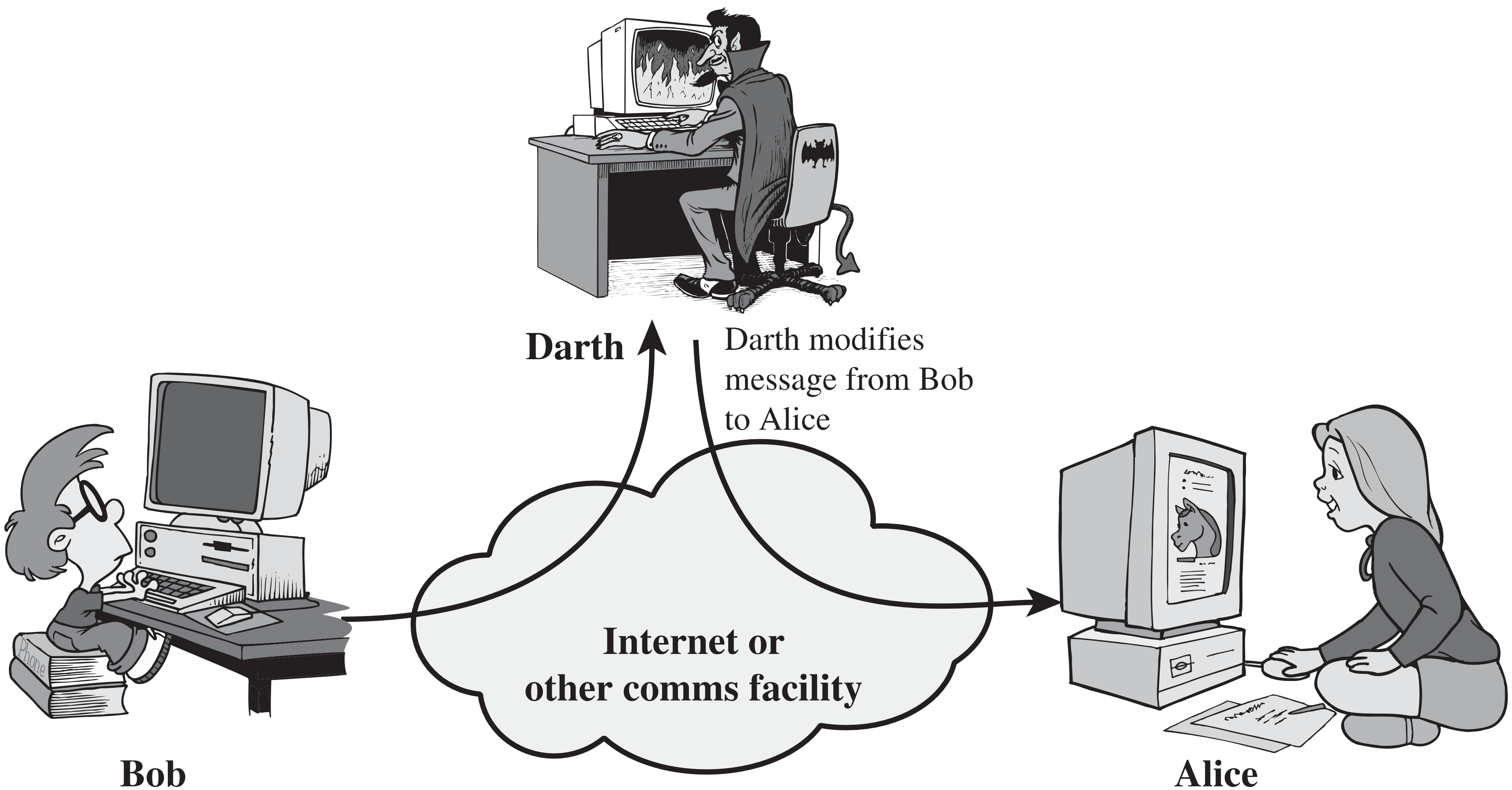
(a) Masquerade

Active Attacks (b)



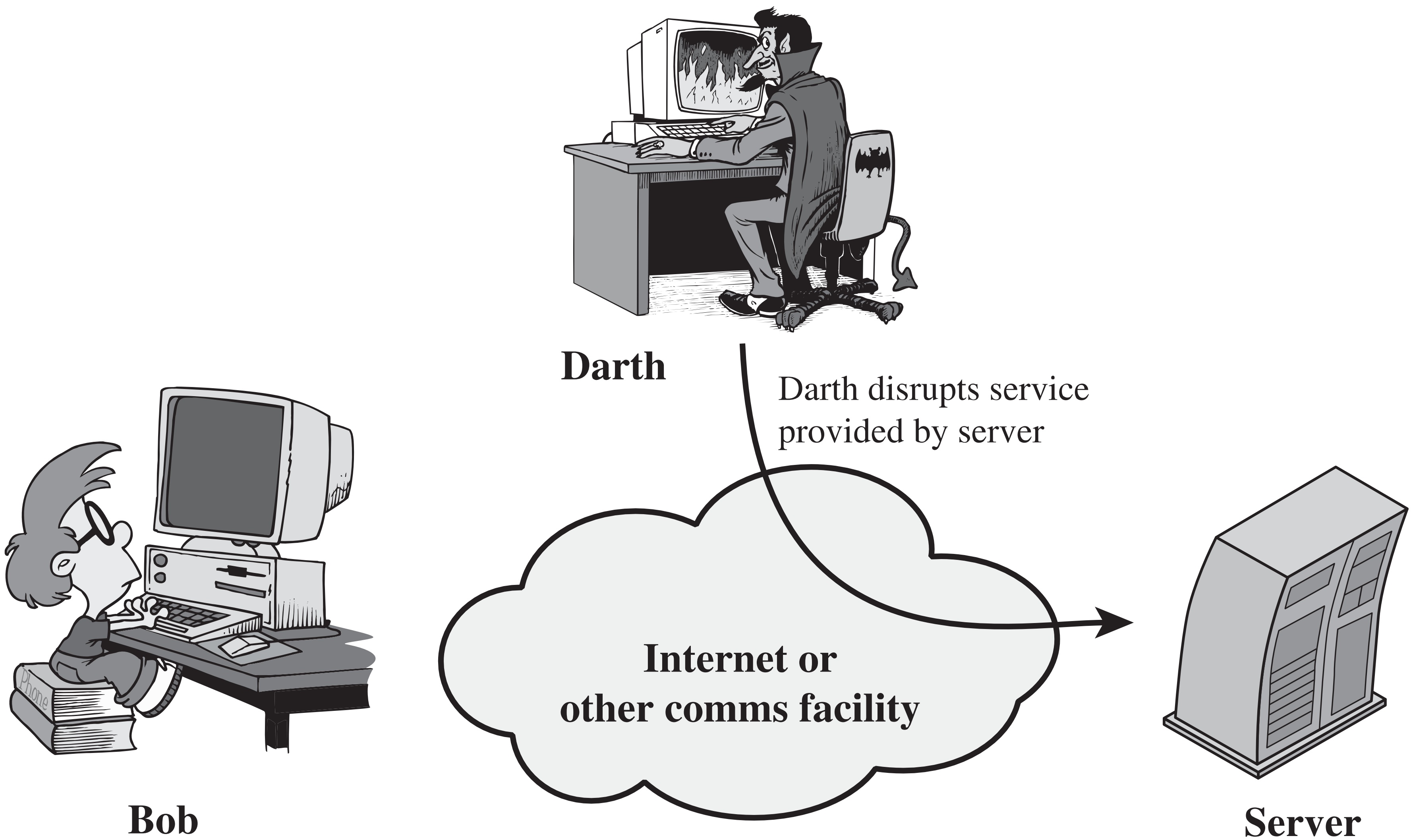
(b) Replay

Active Attacks (c)



(c) Modification of messages

Active Attacks (d)



(d) Denial of service

Response to Attacks

- Identify key assets
- Evaluate threat posed to assets
- Implement suitable countermeasures
- Manage implementation of Security services

Security Services

- Security services normally associated with physical documents
  - Eg. Include signatures, dates; Protect from disclosure, tampering, or destruction; be witnessed; be recorded or licensed, etc.
- Intended to counter security attacks
- Enhances the security of the data processing systems and the information transfers of an organization
- Make use of one or more security mechanisms to provide the security services

Security Services

- International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) X.800 Security Architecture for Open System Interconnection (OSI) defines a systematic way of defining and providing security requirements
- The OSI security architecture is useful to managers as a way of organizing the task of providing security
- It provides a useful overview of concepts

Security Services

- X.800 defines it as:
  - A service provided by a **protocol layer of communicating open systems**, which ensures adequate security of the systems or of data transfers
- RFC 2828 defines it as:
  - A processing or communication service provided by a system to give a specific kind of protection to system resources
- X.800 defines it in 5 major categories

Security Services (X.800)

- **Confidentiality** – protection of data from unauthorized disclosure
- **Integrity** – assurance that data received is as sent by an authorized entity
- **Authentication** – assurance that the communicating entity is the one claimed
- **Access Control** – prevention of the unauthorized use of a resource
- **Non-Repudiation** – protection against denial by one of the parties in a communication

Security Mechanisms

- A mechanism that is designed to detect, prevent, or recover from a security attack
- No single mechanism that will support all functions required
- However one particular element underlies many of the security mechanisms in use: cryptographic techniques (Hence we focus on this area)

Encryption is a key enabling technology.

Security Mechanisms (X.800)

- Specific security mechanisms
  - May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services
  - Decipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, Notarization
- Pervasive security mechanisms
  - Mechanisms that are not specific to any particular OSI security service or protocol layer
  - Trusted functionality, security labels, event detection, security audit trails, security recovery

Security Mechanisms (X.800)

Service	Mechanism: Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Relationship between Security Services and Mechanisms

Security services are implemented by ***security mechanisms!***

Some Cryptography Terms

- **Cryptography**
  - The study of secret (crypto-) writing (-graphy)
  - The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and retransforming that message back to its original form
- **Cryptanalysis** (code-breaking)
  - The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key.
- **Cryptology**
  - The field encompassing both cryptography and cryptanalysis

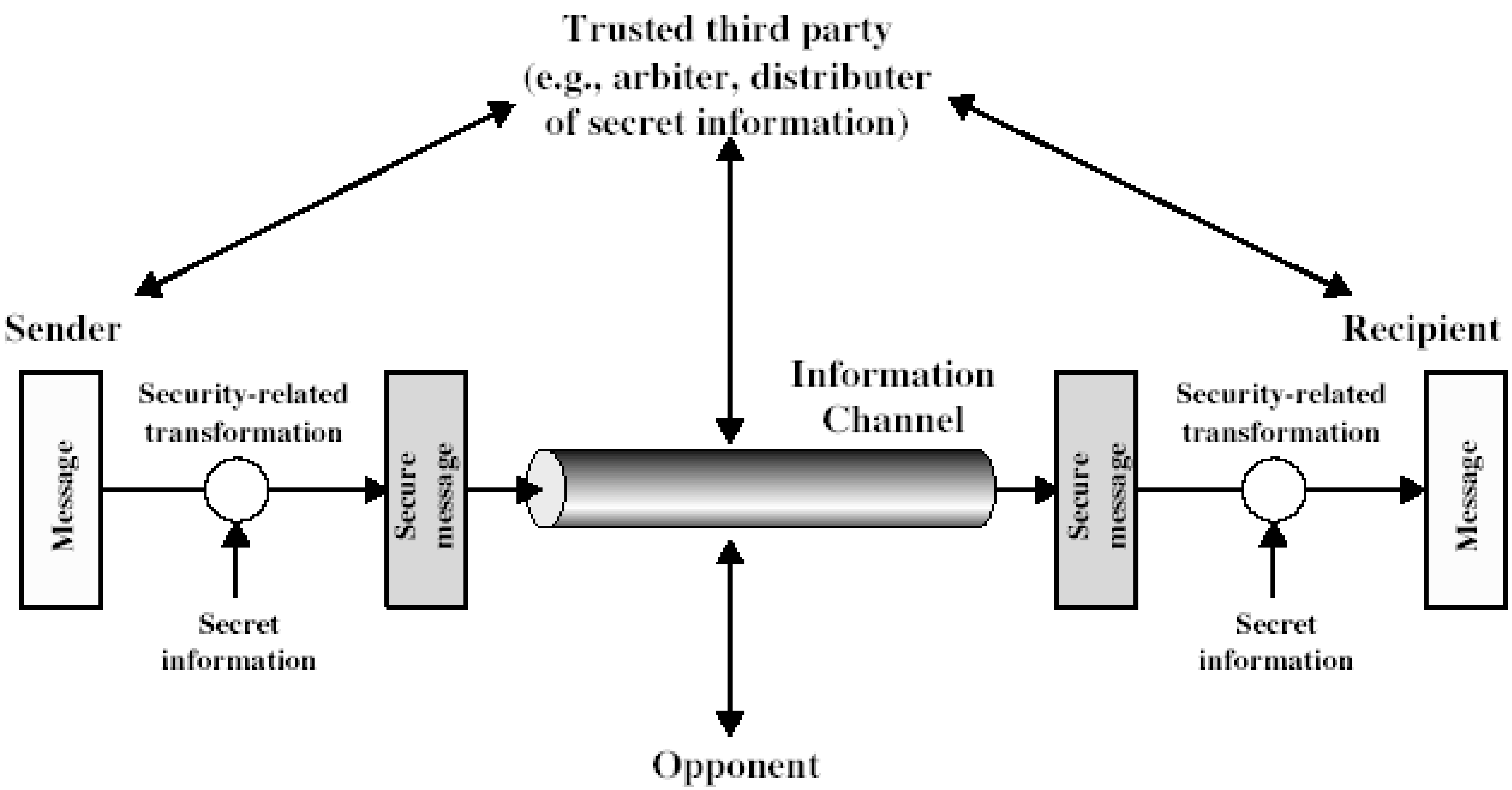
Some Cryptography Terms

- **Cipher**
  - An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods
- **Encipher** (encode)
  - The process of converting plaintext to ciphertext using a cipher and a key
- **Decipher** (decode)
  - The process of converting ciphertext back into plaintext using a cipher and a key

Some Cryptography Terms

- **Encryption**
  - The mathematical function mapping plaintext to ciphertext using the specified key: $C = E_K(P)$
- **Decryption**
  - The mathematical function mapping ciphertext to plaintext using the specified key: $P = E_{K^{-1}}(C)$
- **Plaintext**
  - The original intelligible message
- **Ciphertext**
  - The transformed message
- **Key** (Password)
  - Some critical information used by the cipher, known only to the sender & receiver

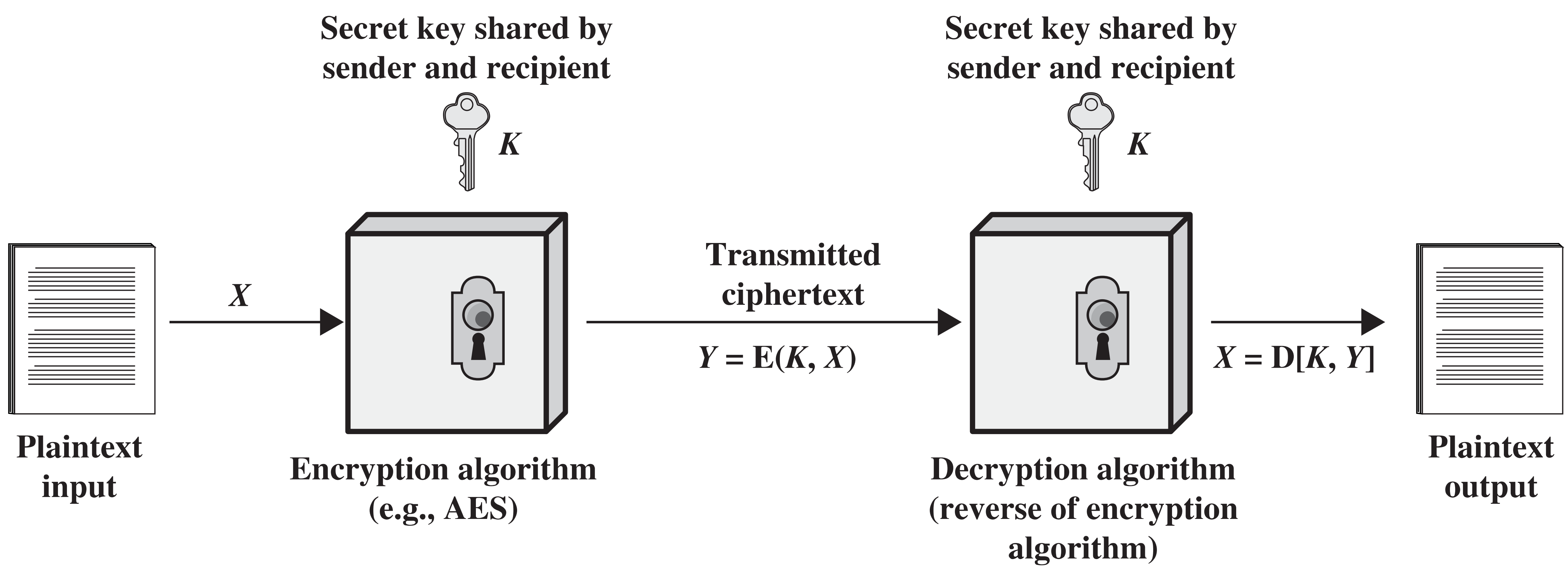
Model for Network Security



Model for Network Security

- Using this model, four basic tasks are required in designing a particular security service:
  - Design an **algorithm** for the security transformation
  - Generate the **secret information** used by the algorithm
  - Develop **methods** to distribute the secret information
  - Specify a protocol enabling the two principals to use the transformation & secret info for a security service

Symmetric Cipher Model

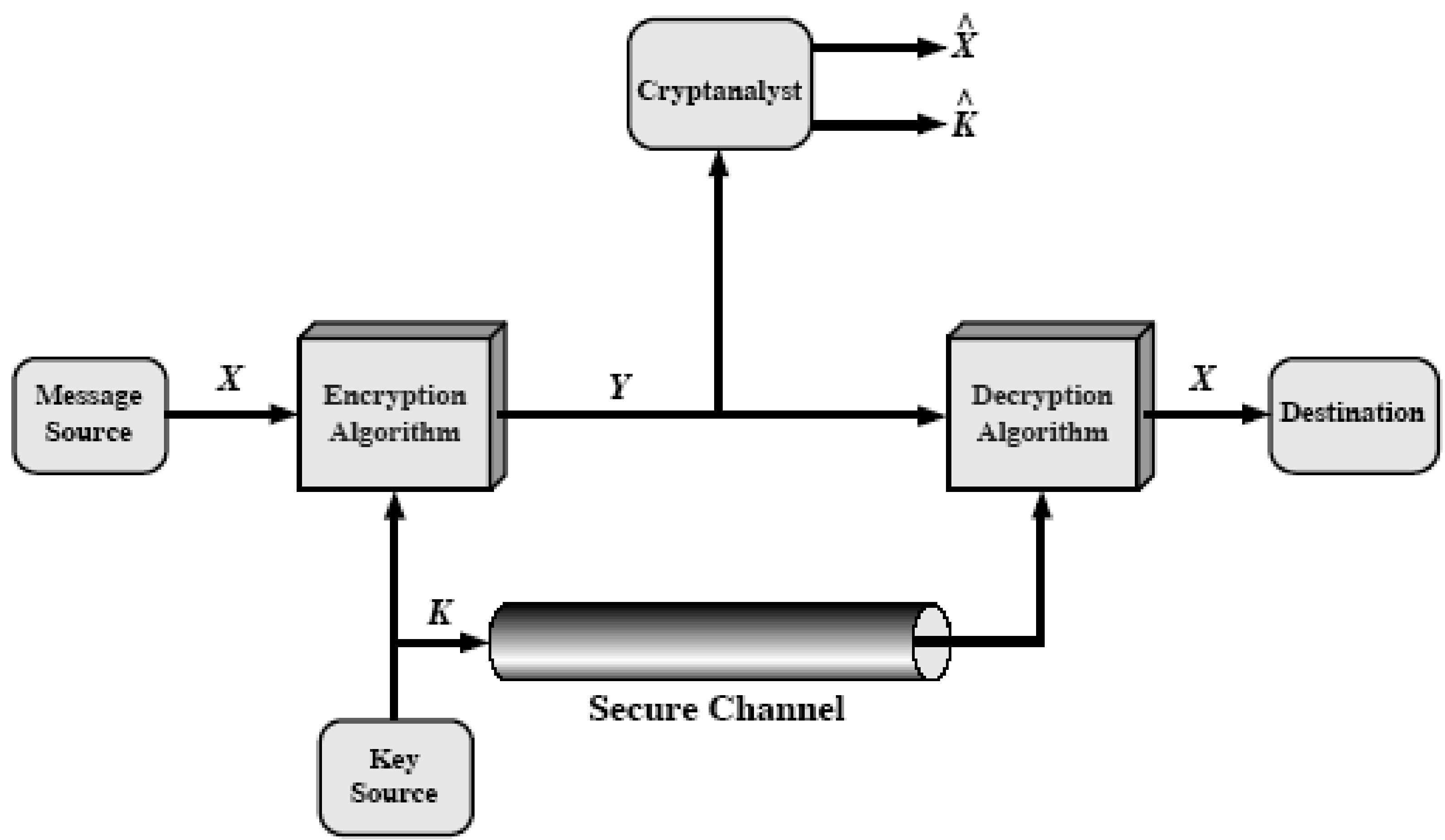


Symmetric Cipher Model

- A symmetric encryption scheme has five ingredients:
  - **Plaintext**: This is the original intelligible message or data that is fed into the algorithm as input.
  - **Encryption algorithm**: The encryption algorithm performs various substitutions and transformations on the plaintext.
  - **Secret key**: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.
  - **Ciphertext**: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
  - **Decryption algorithm**: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Conventional Encryption Algorithms

- A private-key (or secret-key, or single-key) encryption algorithm is one where the sender and the recipient share a common key.
- Traditional encryption algorithms are private-key



Key

- The parameter which selects which individual transformation is used, and is selected from a keyspace K.
- More formally we can define the cryptographic system as a single parameter family of invertible transformations.
- $C = E_k$; k in $K : P \rightarrow C$
- $P = E_k^{-1}$; k in $K : C \rightarrow P$

Exhaustive Key Search

- It is also called ***Brute-force attack*** that is always theoretically possible to simply try every key
- Most basic attack, directly proportional to *key size*. It is the attack we would assume.
- Assume either know or can recognize when plaintext is found
- Tabulate for reasonable assumptions about number of operations possible

Exhaustive Key Search

Key Size (bits)	No. of keys	Time (1 encryption/μs)	Time (10^6 encryptions/μs)
32	$2^{32} = 4.3 \times 10^9$	35.8 minutes	2.15 millisec
56 (DES)	$2^{56} = 7.2 \times 10^{16}$	1142 years	10.01 hours
128 (AES)	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{24} years	5.4×10^{18} years
168 (3DES)	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{36} years	5.9×10^{30} years
26 characters permutation	$26! = 4 \times 10^{26}$	6.4×10^{12} years	6.4×10^6 years

Unconditional and Computational Secure

- Unconditional secure
  - No matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext.
- Computational secure
  - Given limited computing resources (e.g. time needed for calculations is greater than age of universe), the cipher cannot be broken
    - Cost of breaking exceeds the value of information
    - Time required exceeds the lifetime of information

Classical Ciphers

- Two basic components in classical ciphers:
  - Substitution ciphers by replacing letters
    - Caesar cipher
    - Monoalphabetic cipher
    - Vigenère cipher
  - Transposition ciphers by arranging letters in a different order
- Several such ciphers may be concatenated together to form a product cipher

Caesar Cipher

- Firstly used in military affairs (Gallic wars)
- Replace each letter by a shift operation from 1 to 25
- Mathematically expressed as the function:
  - Assign A to value 0, B=1, C=2, ... Y=24, Z=25
  - Encryption is done using
    - E_k: i → i + k (mod 26)
  - Decryption is done using
    - D_k: i → i - k (mod 26)

Cryptanalysis – Brute Force

- Each alphabet is mapped to another alphabet by shifting each to the left or right circularly
- Could simply try each in turn by an exhaustive key search
- Given some ciphertext, just try every shift of letters:
- `lizhzlvkwruhsodfhohwwhuv` original ciphertext
  `khygykujvqtgrncegngvvgtu` try shift of 1
  `jgxfxjtiupsfqmbdfmfuufst` try shift of 2
  `ifwewishtoreplaceletters` try shift of 3 *
  `hevdvhrgsnqdokzbdkdssdqr` try shift of 4
  `gducugqfrmpcnjyacjcrrcpq` try shift of 5
  .....
  `mjaiamwlxsvitpegipixxivw` try shift of 25

Cryptanalysis – Brute Force

- Three important characteristics
  - Encryption and decryption algorithm are known
    - The trend
  - Key space is 25
    - Too small for brute-force
  - Language of plaintext is known and easily recognizable
    - If language of plaintext is unknown, the plaintext output may not be recognizable
    - Commonly use compression

Monoalphabetic Cipher

- Rather than just shifting the alphabet, we could shuffle the letters arbitrarily
- Each plaintext letter maps to a different random ciphertext letter
- The key is 26 letters long
- Suppose we have the key below
  - Plain: abcdefghijklmnopqrstuvwxyz
  - Cipher: dkvqfibjwpescxhtmyauolrgzn

  - Plaintext: if we wish to replace letters
  - Ciphertext: wi rf rwaj uh yftsdvf sfuufya

Monoalphabetic Cipher

- A very large key space
  - Total number of keys is 26! ~ 4×10^{26}
- Secure?
- But would be !!!WRONG!!!
  - Problem is the language characteristic

Language Redundancy

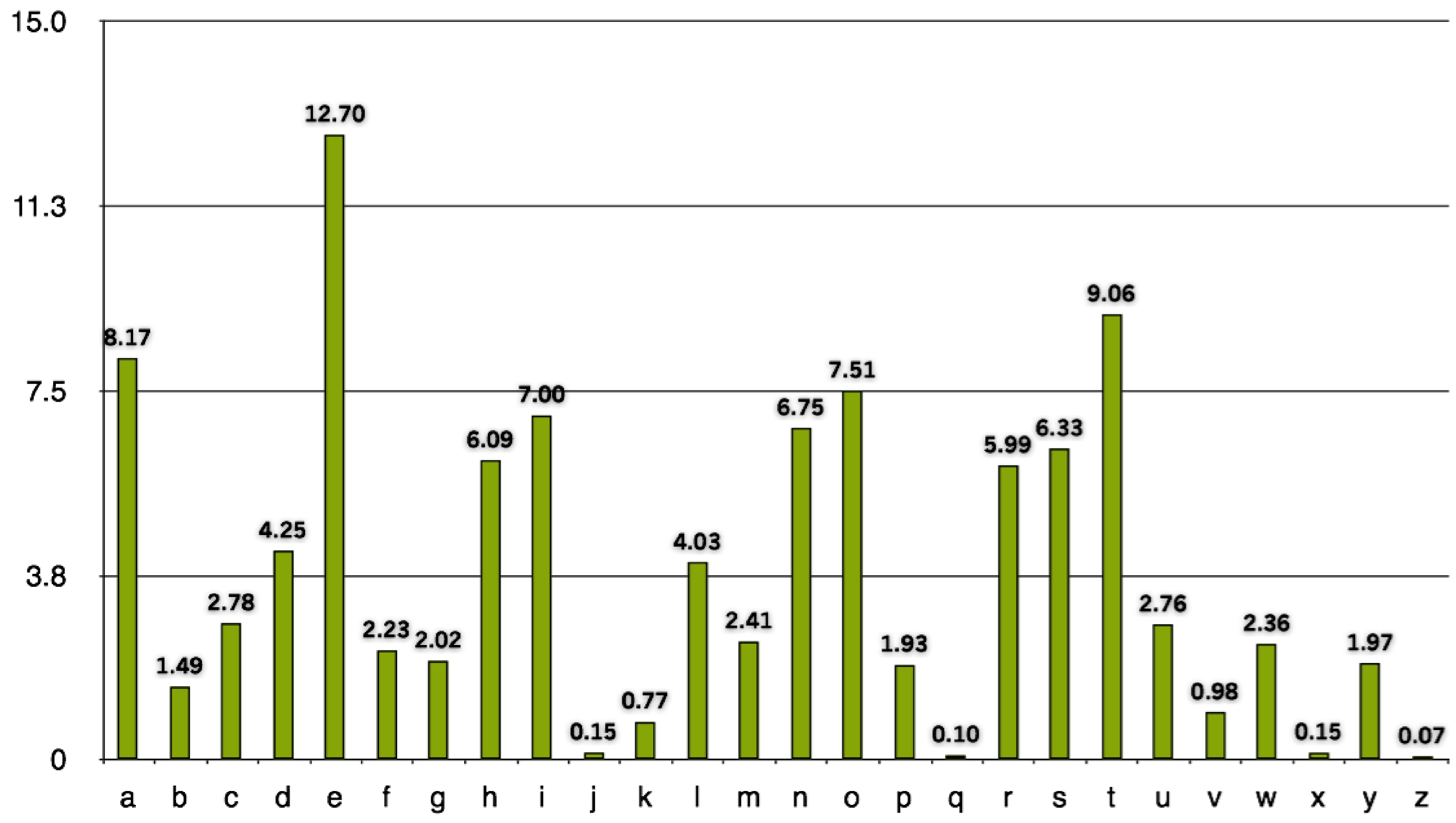
- Human languages are redundant (Eg., the, is, etc)
- Letters are not equally commonly used
- In English e is by far the most common letter
  - then T, R, N, I, O, A, S
- Other letters are fairly rare (such as z, j, k, q, x)
- Have tables of single, double & triple letter frequencies

English Letter Frequencies (%)

A	8.167	N	6.749
B	1.492	O	7.507
C	2.782	P	1.929
D	4.253	Q	0.095
E	12.702	R	5.987
F	2.228	S	6.327
G	2.015	T	9.056
H	6.094	U	2.758
I	6.996	V	0.978
J	0.153	W	2.360
K	0.772	X	0.150
L	4.025	Y	1.974
M	2.406	Z	0.074

Single	Double	Triple
E	TH	THE
T	HE	AND
R	IN	TIO
N	ER	ATI
I	RE	FOR
O	ON	THA
A	AN	THE
S	EN	RES

English Letter Frequencies (%)



Cryptanalysis – Statistical Attack

- Key concept - Monoalphabetic substitution does not change relative letter frequencies
- Calculate letter frequencies for ciphertext being analyzed
- Compare counts/plots against known values
- In particular look for common peaks and troughs
- Peaks at: AEI spaced triple, NO pair, RST triple with U shape; Troughs at: JK, XZ

Cryptanalysis – Statistical Attack

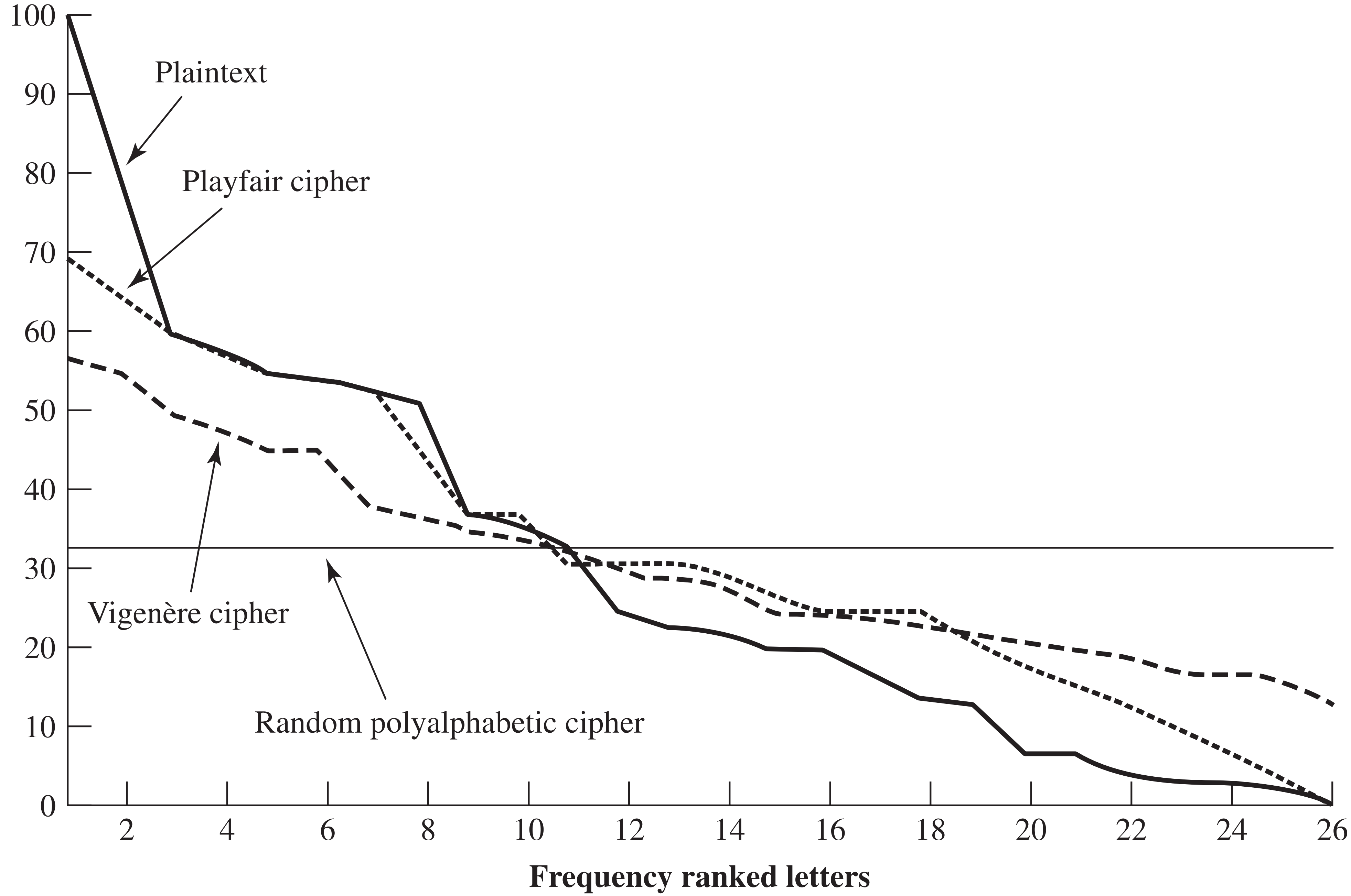
- Analyze the letter frequency.
- Given "JXU WHUQJUIJ TYISELUHO EV CO WUDUHQJYED YI JXQJ Q XKCQD RUYDW SQD QBJUH XYI BYVU RO QBJUHYDW XYI QJJYJKTUI".
- Count letters and plot as below.

```
                                      E
                * T            A      *
                *                     *        I
                *             *       *       *
                *             *       *       *
    N         S *             *       *       *
    *       R * *             *       *       *
    *       * * *             *       *     * *
    *       * * *             *       *   * * *
*   * *     * * *         *   *       *   * * *
* * * *     * * * *       *   * * * * * * * * *
* * * *     * * * * *     *   * * * * * * * * *
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
```

Cryptanalysis – Statistical Attack

- Looking at this graph
  - The `A-E-I` triple is pretty clear at `Q-U-Y`
  - `HIJ` triple would fit as `RST`, `DE` is `NO`, …
- Try out any possible substitution that will produce a reasonable output

Cryptanalysis – Statistical Attack



Vigenère Cipher

52

- Vigenère cipher is a multiple Caesar cipher
- Key is multiple letters long $K = k_1, k_2, \ldots, k_n$
- i^{th} letter specifies i^{th} alphabet to use
- Use each alphabet in turn
- Repeat from start after n letters in message
- Mathematically:
  - Encryption: $E_{ki}(a)$: $a \rightarrow a + k_i \pmod{26}$
  - Decryption: $D_{ki}(a)$: $a \rightarrow a - k_i \pmod{26}$

Vigenère Example

- Given a keyword Cipher
  - Plaintext:

    THISPROCESSCANALSOBEEXPRESSED
  - Keyword:

    CIPHERCIPHERCIPHERCIPHERCIPHE
  - Ciphertext:

    VPXZTIQKTZWTCVPSWFDMTETIGAHLH

```
         ABCDEFGHIJKLMNOPQRSTUVWXYZ
C  ->  CDEFGHIJKLMNOPQRSTUVWXYZAB
I  ->  IJKLMNOPQRSTUVWXYZABCDEFGH
P  ->  PQRSTUVWXYZABCDEFGHIJKLMNO
H  ->  HIJKLMNOPQRSTUVWXYZABCDEFG
E  ->  EFGHIJKLMNOPQRSTUVWXYZABCD
R  ->  RSTUVWXYZABCDEFGHIJKLMNOPQ
         ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Improvement (Polyalphabetic Cipher)

54

- An approach to improving security is to use multiple cipher alphabets, hence the name polyalphabetic ciphers.
  - Vigenère cipher, which is a multiple Caesar cipher.
- Flattens frequency distribution by using a key to select which alphabet is used for each letter of the message.
  - Make all alphabets to have same frequency distribution.

One-Time Pad

- An unbreakable scheme that using a random key that was truly as long as the message, with no repetitions is known as one-time pad
- Strong because the ciphertext contains no information whatsoever about the plaintext
- Problems:
  - Impractical to generate a large quantities of random keys
  - Key distribution and protection as a key of equal length is needed.

Transposition Ciphers

- Transposition(permutation) ciphers hide the message by rearranging the order of letters in the plaintext
- It does not alter the actual letters
- Ciphertext has the same frequency distribution as the plaintext

Rail Fence Cipher

- Encryption
  - By writing letters in the plaintext on alternate rows
  - Read off cipher row by row
- Example
  - Plain: Meet me after the party

```
m e m a t r h p r y
 e t e f e t e a t
```

  - Cipher: `mematrhpryetefeteat`
- Decryption is a reverse of the encryption
- What about the key?

Row Transposition Ciphers

- It would be more secure by performing more than one transposition
- Example
  - Key:
  - Plaintext:

Key:	4	3	1	2	5	6	7
Plaintext:	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	n	l	y	p	e	t	z

  - Ciphertext:

`nscy auop ttwl tmdn aoie paxt tokz`

Row Transposition Ciphers

- Encryption
  - Write the plaintext in a matrix, row by row
  - Read the plaintext off, column by column, based on the order specified in the key
- Example
  - Key: `4 3 1 2 5 6 7`
  - Plaintext:

4	3	1	2	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

  - Ciphertext: `ttna aptm tsuo aodw coix knly petz`
- Decryption is a recovery of the matrix based on the key
- Cryptanalysis involves laying out the ciphertext in a matrix and playing around with column positions.