Cryptography & Security

Santosh Chapaneri,
Assistant Professor, EXTC, SFIT

Outline

- What is Cryptography?
- Goals, Attacks
- Symmetric Encryption
- Number Theory
- Public Key Cryptography, RSA
- Applications
- Security
  - Malicious programs
  - Counter-measures

What is Cryptography?

- Did you use any form of Cryptography
  - Last week?
  - Last month?
  - Last year?

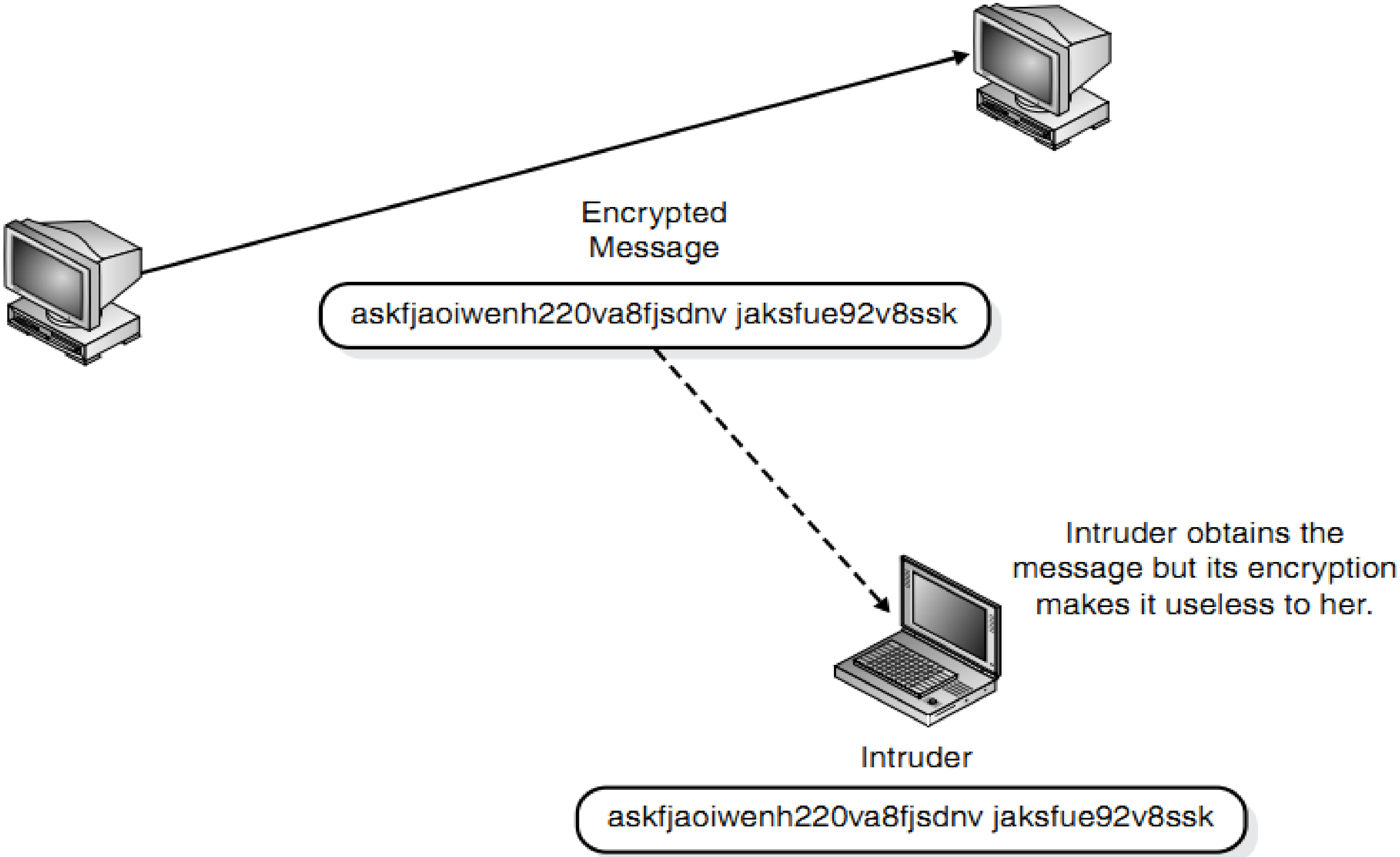
What is Cryptography?

- https invokes the Secure Socket Layer (SSL) communication security protocol to securely transmit your credit card number to the server
- SSL uses cryptography

What is Cryptography?

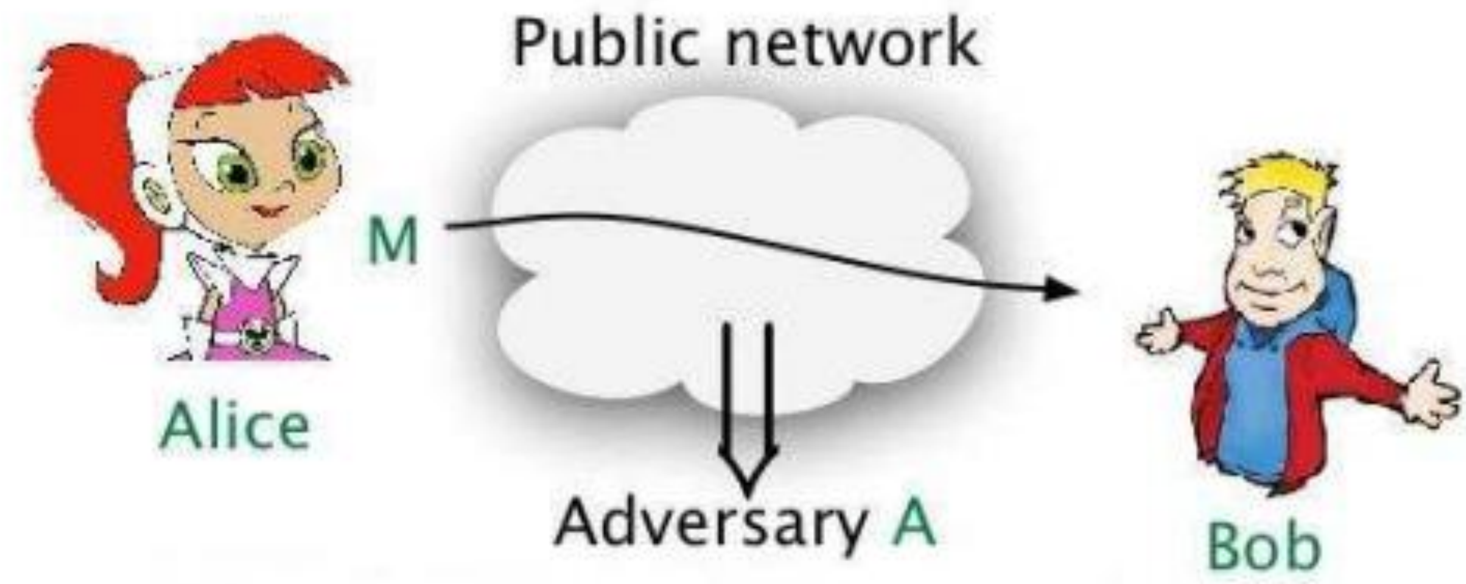
- Other usage of Cryptography
  - ATM machines
  - Online banking
  - Electronic Signatures
  - etc…

How does Cryptography help you?



Without the right key, the captured message is useless to an attacker.

What is Cryptography about?

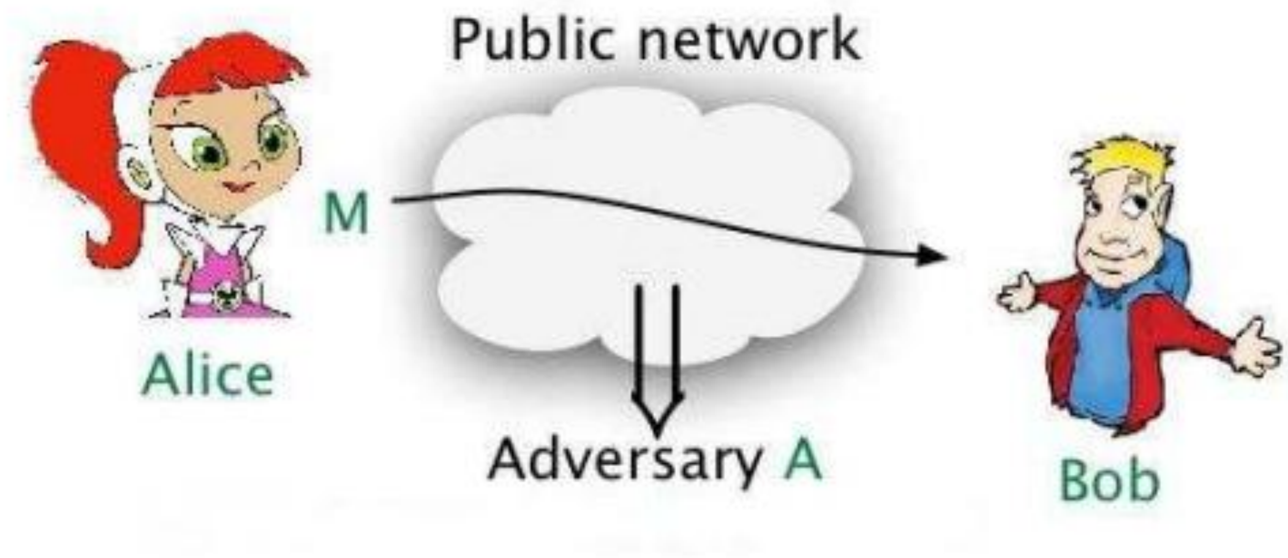


Adversary: clever person with powerful computer

Goals:

- Data privacy
- Data integrity and authenticity

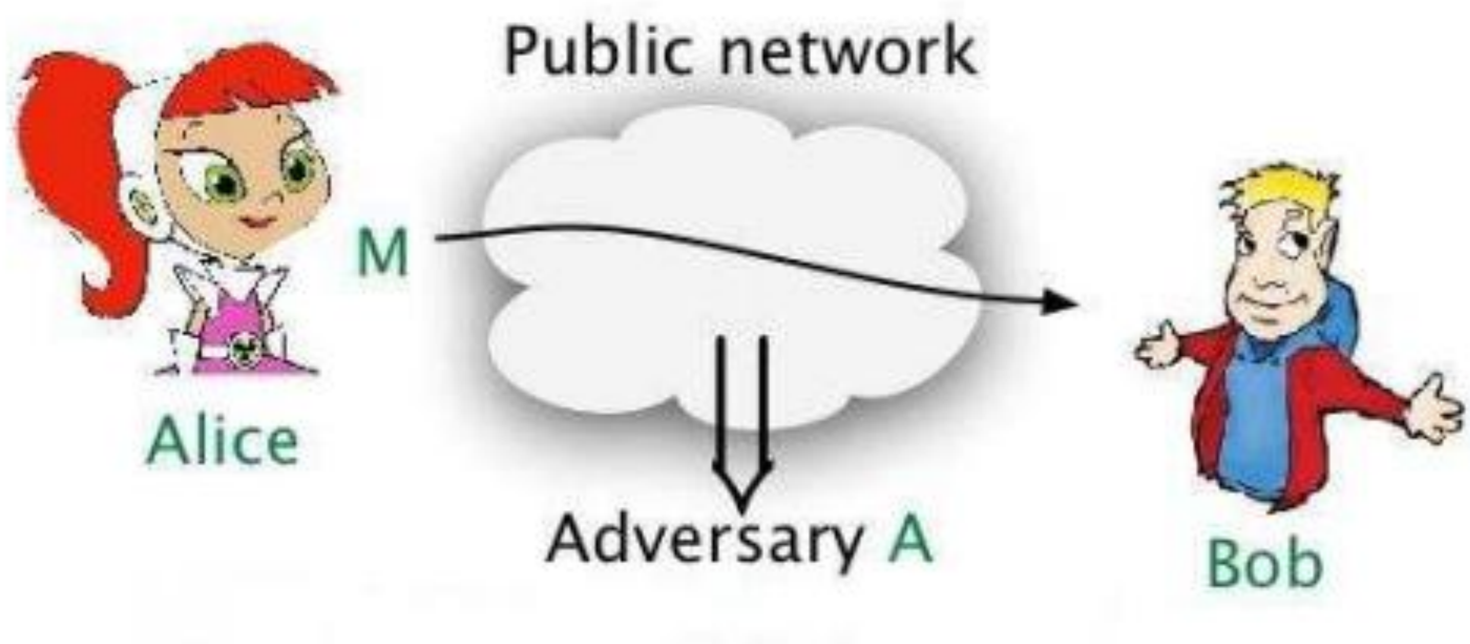
Data Privacy



The goal is to ensure that the adversary does not see or obtain the data (message) M.

Example: M could be a credit card number being sent by shopper Alice to server Bob and we want to ensure attackers don't learn it.

Data Integrity & Authenticity



The goal is to ensure that

- *M* really originates with Alice and not someone else
- *M* has not been modified in transit

Example of Attack

Alice

Bob
(Bank)

Alice

Pay $100 to Charlie

Adversary Eve might

- Modify "Charlie" to "Eve"
- Modify "$100" to "$1000"

Integrity prevents such attacks.

Terminology

- **Plaintext** – original message
- **Ciphertext** – encrypted message
- **Cipher** – algorithm for transforming plaintext to ciphertext
- **Key** – Info used in cipher known only to sender/receiver
- **Encryption** – Converting plaintext to ciphertext
- **Decryption** – Recovering ciphertext from plaintext
- **Cryptography** – Study of encryption principles/methods
- **Cryptanalysis (Code-breaking)** – Study of principles/ methods of deciphering ciphertext ***without*** **knowing the key**
- **Cryptology** – Field of both Cryptography and Cryptanalysis
- **Attack** – An assault on system security to **evade security services and violate the security policy of a system**

Types of Attacks

- **Passive & Active attacks**

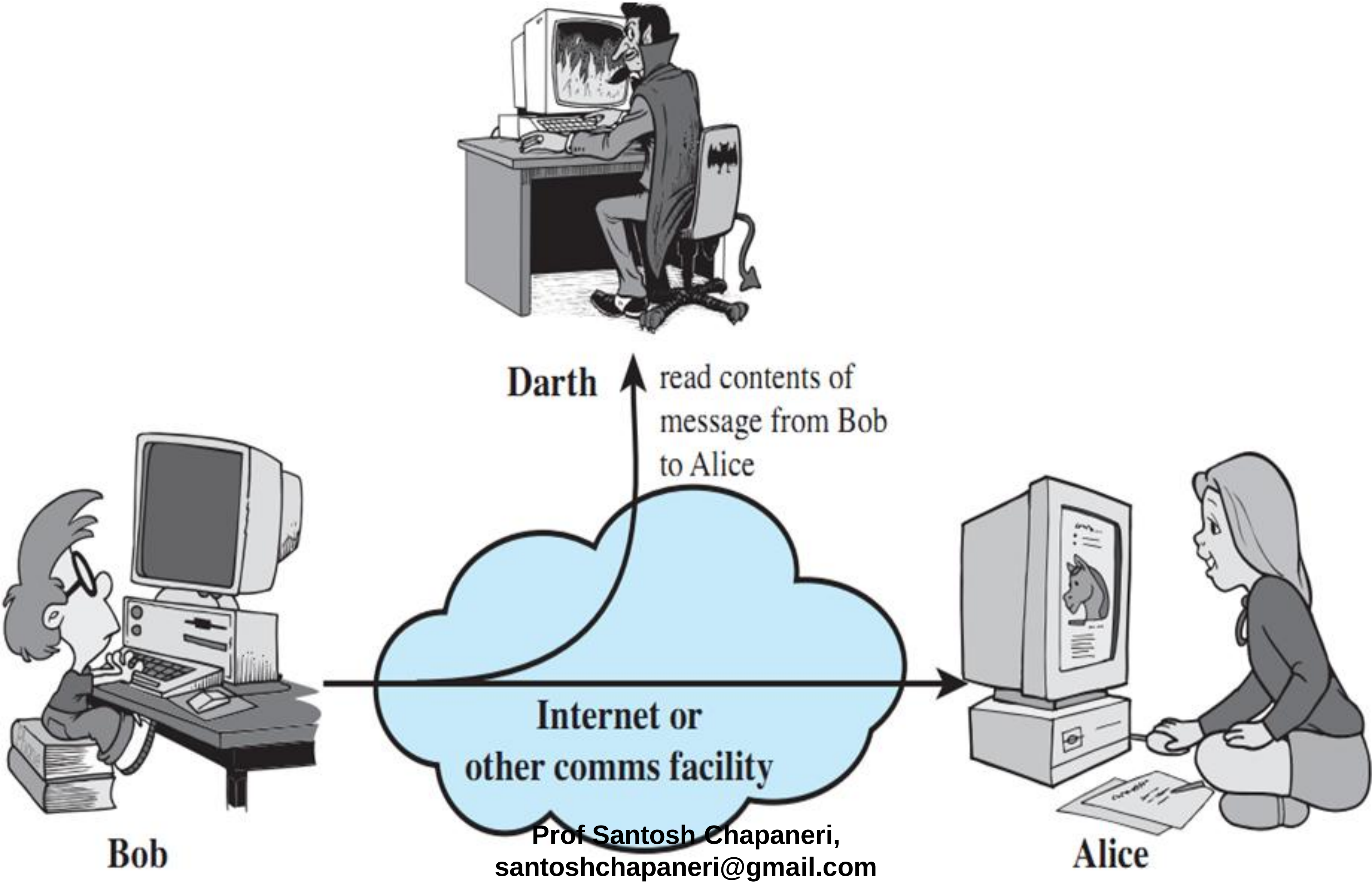
- **<u>Passive Attacks</u>**: Passive attacks are in the nature of **eavesdropping** on, or **monitoring** of transmissions.
- The goal of the opponent is to **obtain information** that is being transmitted. Two types of passive attacks are

  a) release of message contents: and

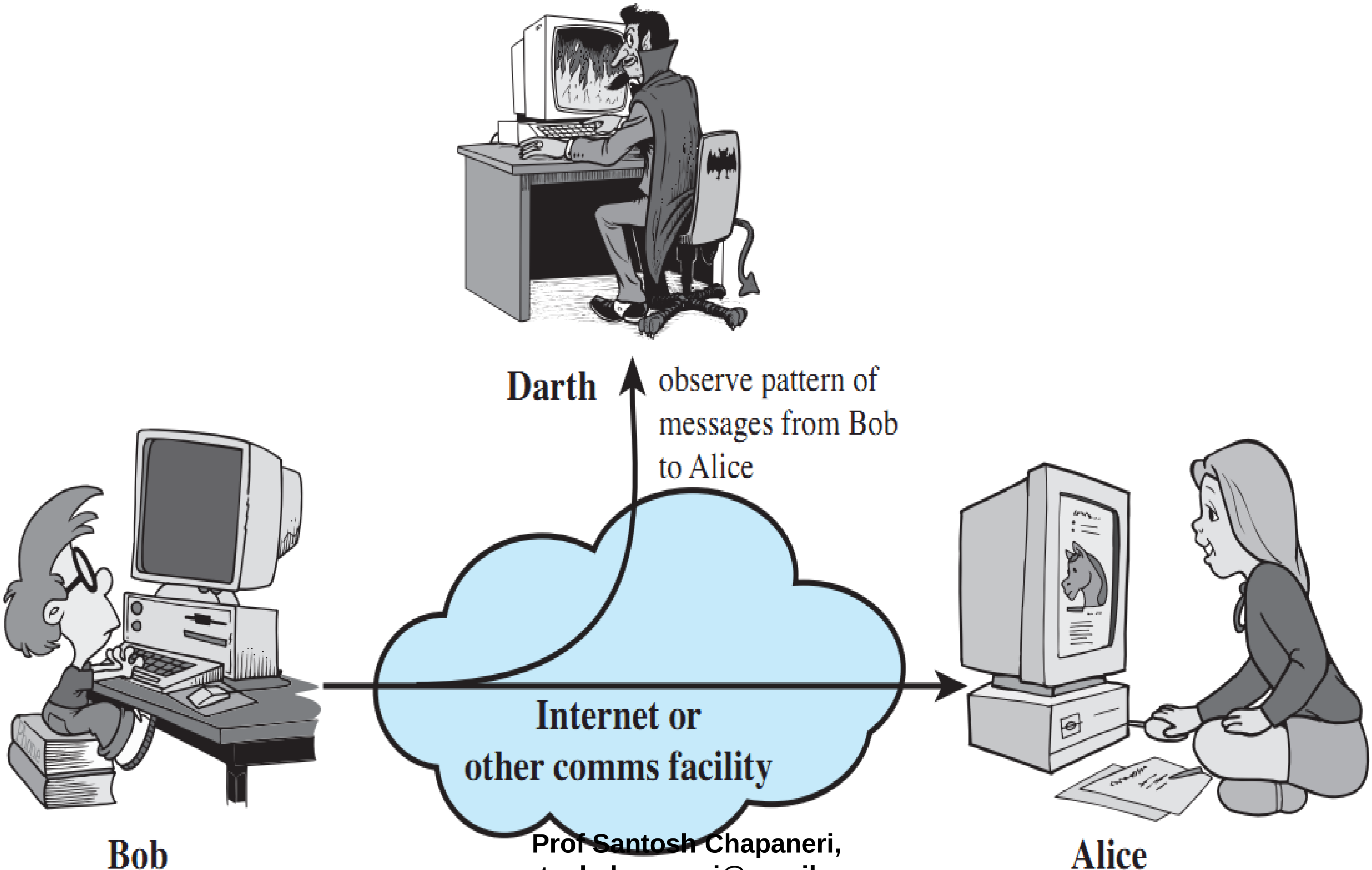
  b) traffic analysis:

- These attacks are difficult to detect because they **do not involve any alteration** of the data.

Passive Attacks: Release of Message Contents



Passive Attacks: Traffic Analysis



Active Attacks

- **Active Attacks**: Active attacks involve some modification of the data stream

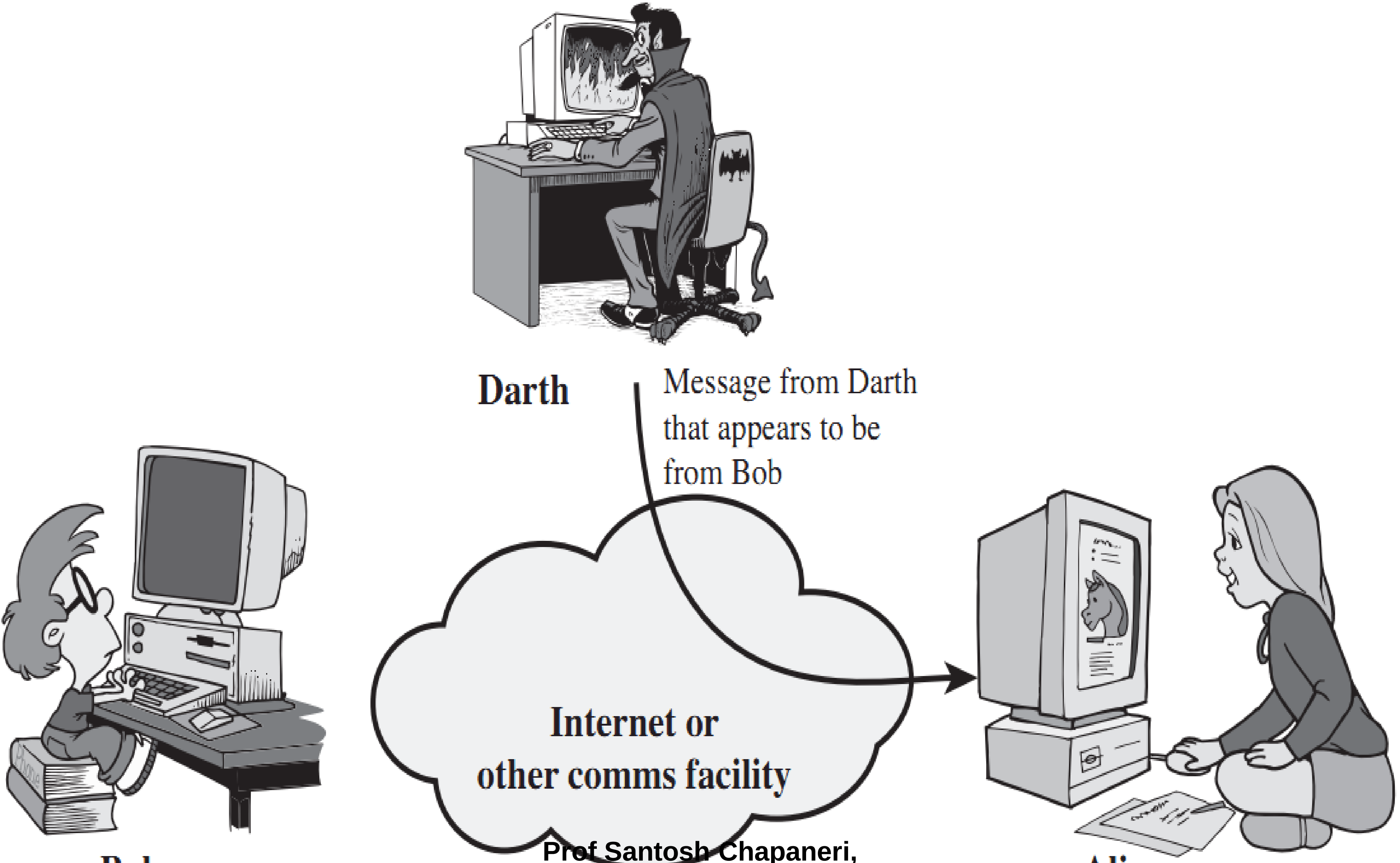
  a) A **masquerade** takes place when one entity pretends to be a different entity.

  b) A **replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

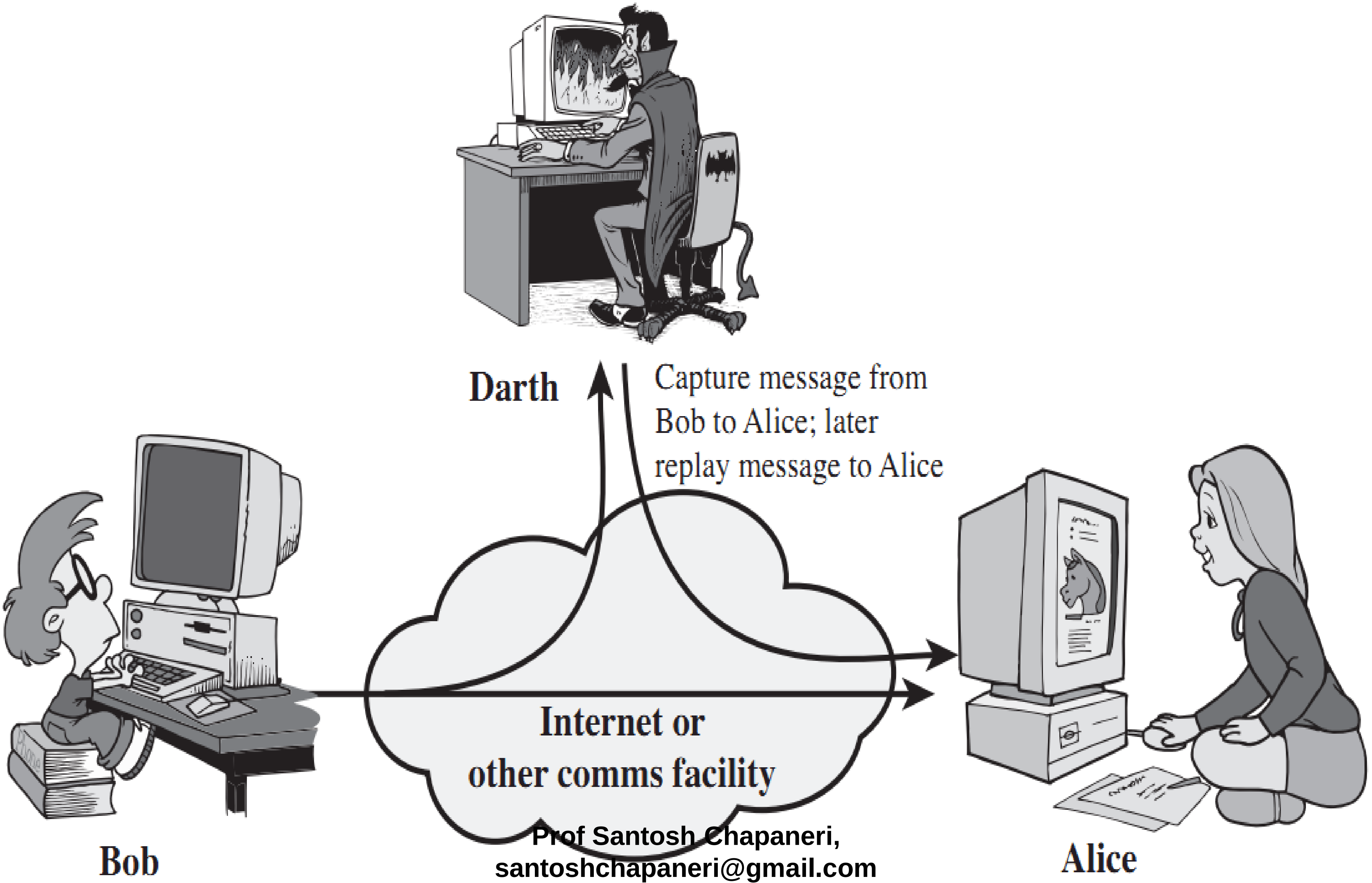
  c) **Modification of messages** means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

  d) The **denial of service** prevents or inhibits the normal use or management of communications facilities.

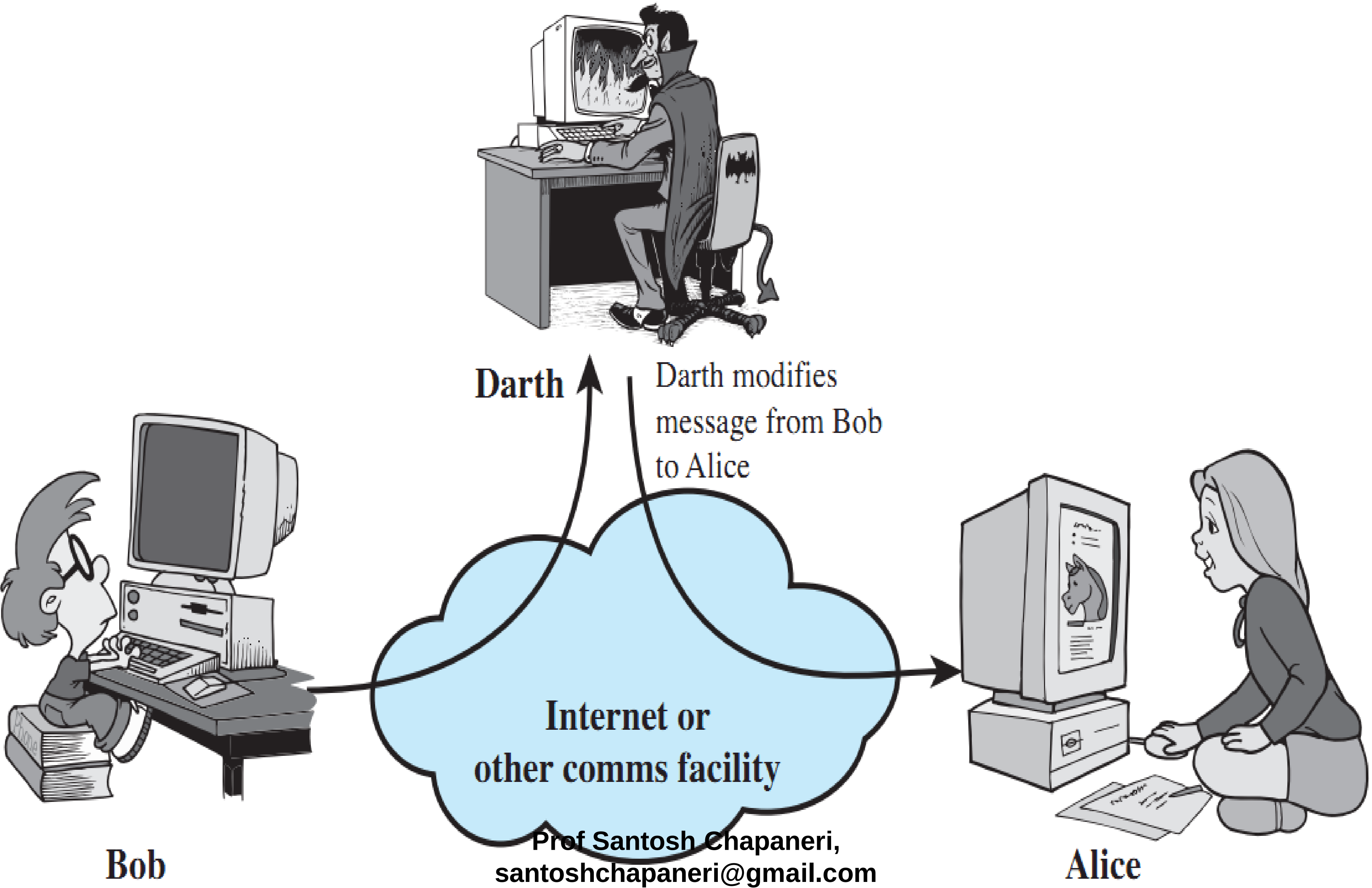
Active Attacks: Masquerade



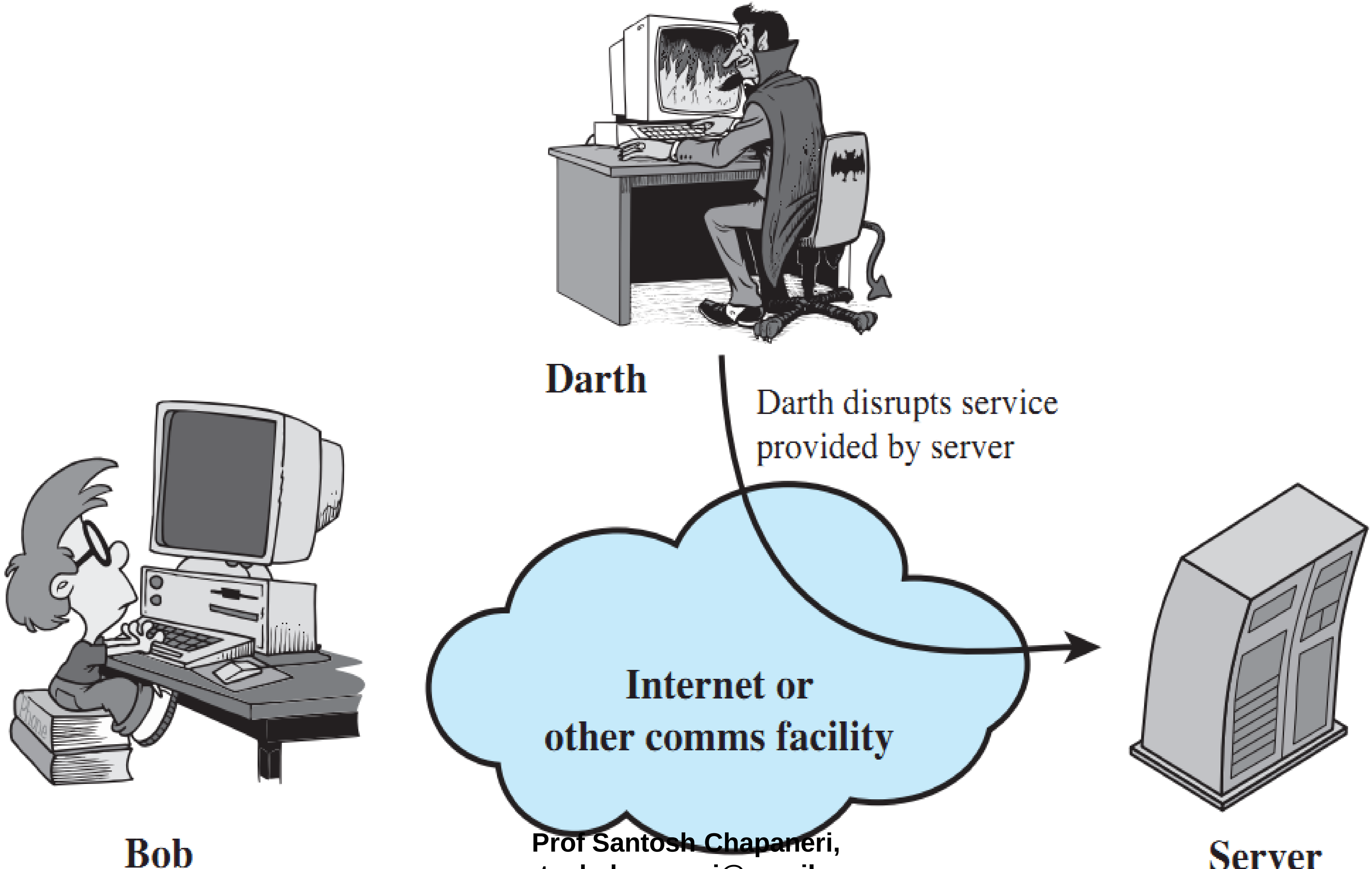
Active Attacks: Replay



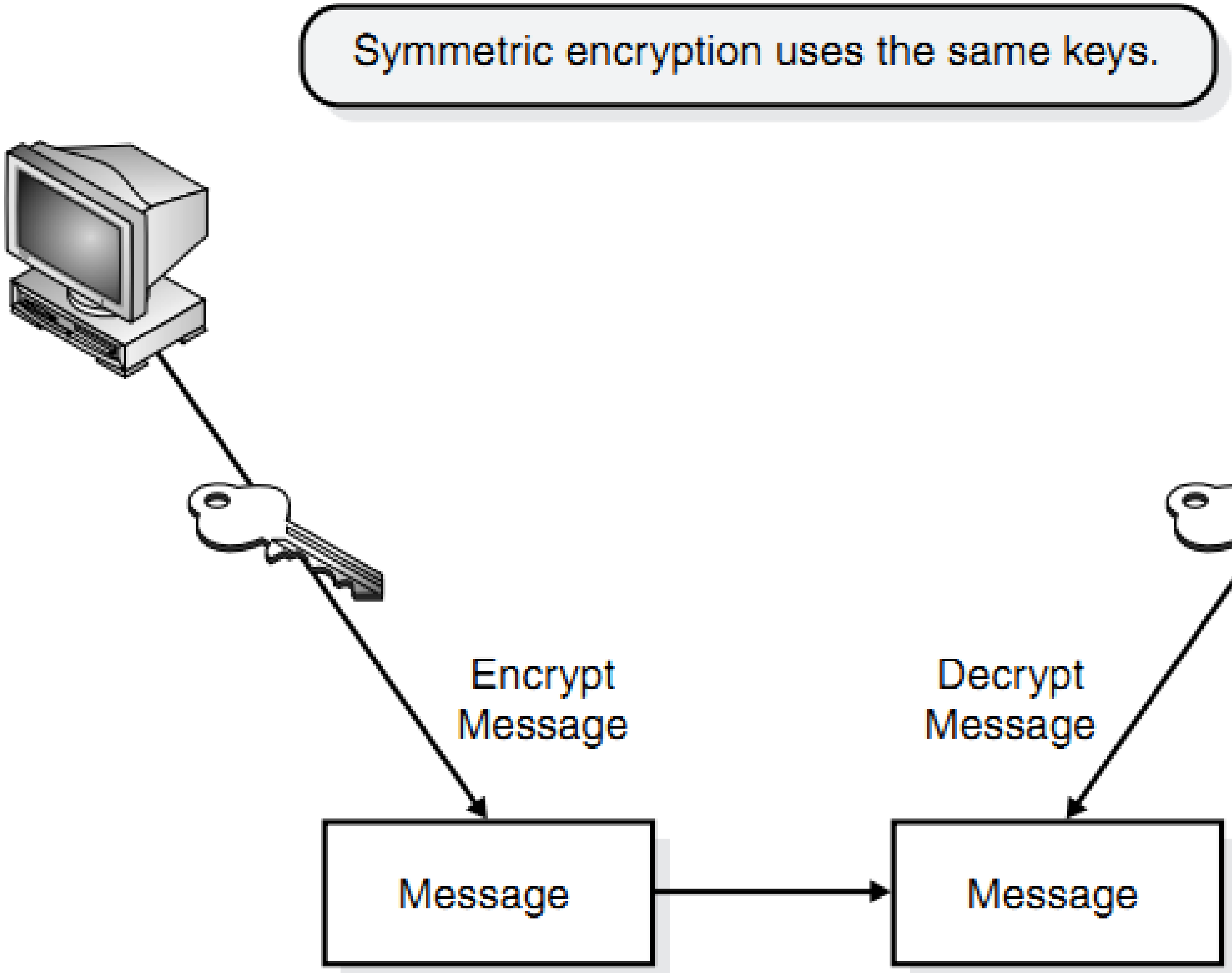
Active Attacks: Modification of Messages



Active Attacks: Denial of Service

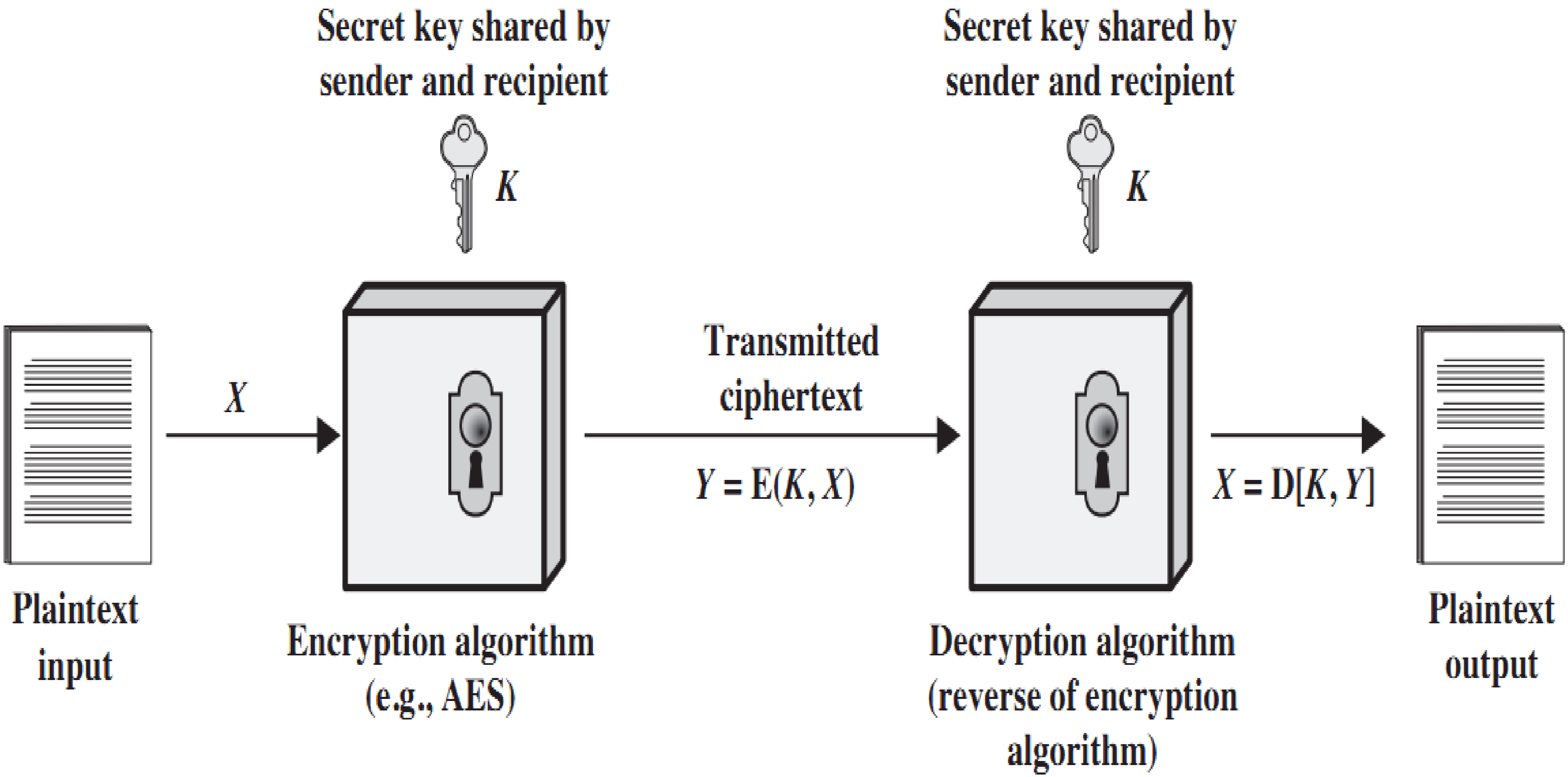


Symmetric (Conventional) Cryptography



Symmetric (Conventional) Cryptography

- Also known as private key / single key cryptography
- Sender and Recipient share a ***common private key***



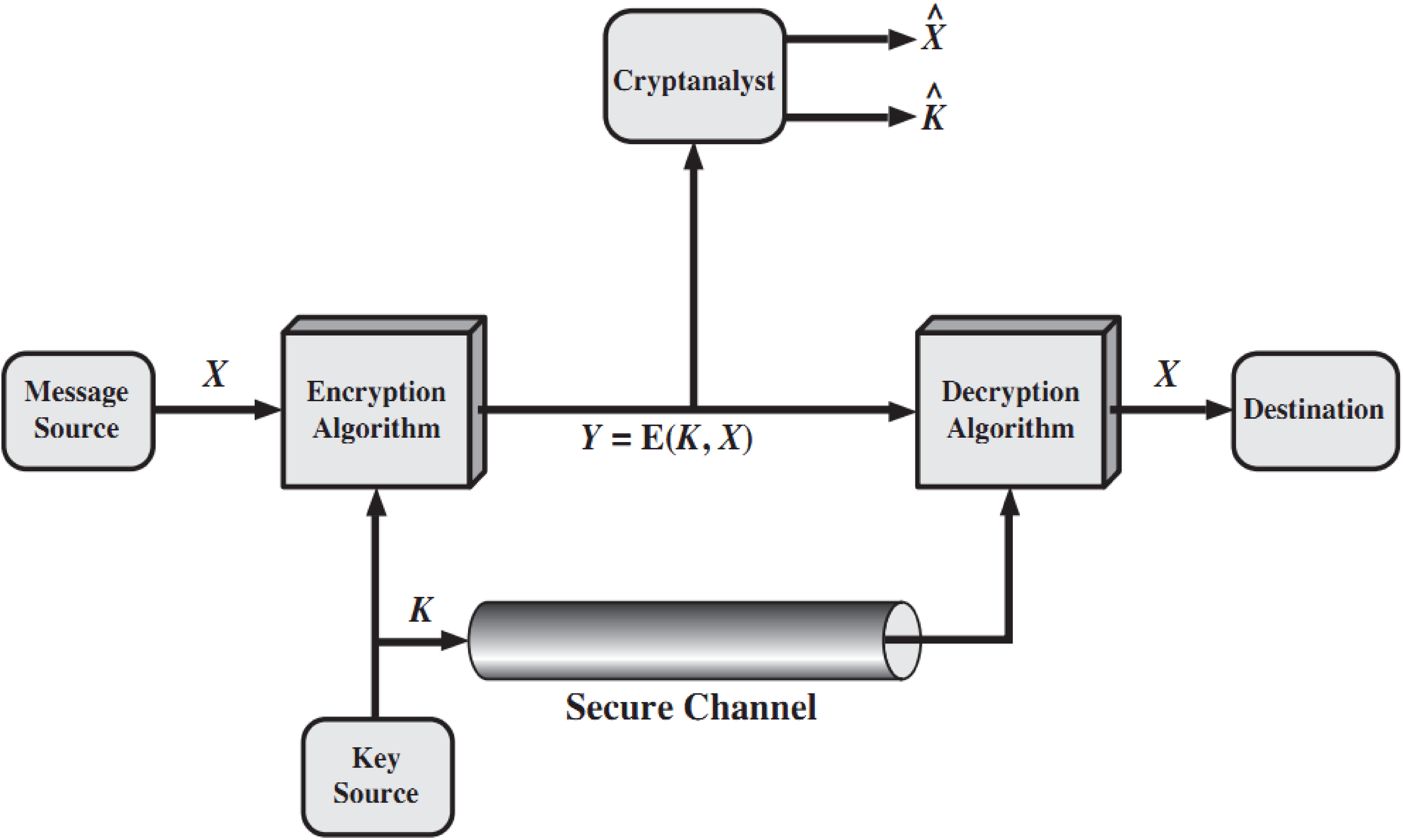
Requirements: Symmetric Cryptography

- Two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- Mathematically, we have:

$$Y = E(K, X) \text{ and } X = D(K, Y)$$

- Assume encryption algorithm is known to everyone; Implies a secure channel to distribute key
- The intended receiver, in possession of the correct key, is able to invert the transformation.
- An opponent, observing Y but not having access to K or X, may **attempt** to recover X or K.

Model: Symmetric Cryptography



Early History

Substitution ciphers/Caesar ciphers:

$$K_e = K_d = \pi : \Sigma \to \Sigma, \text{ a secret permutation}$$

e.g., $\Sigma = \{A, B, C, \ldots\}$ and π is as follows:

σ	A	B	C	D	$\cdots$
$\pi(\sigma)$	E	A	Z	U	$\cdots$

Problem:
Not very secure

(Common newspaper puzzle)

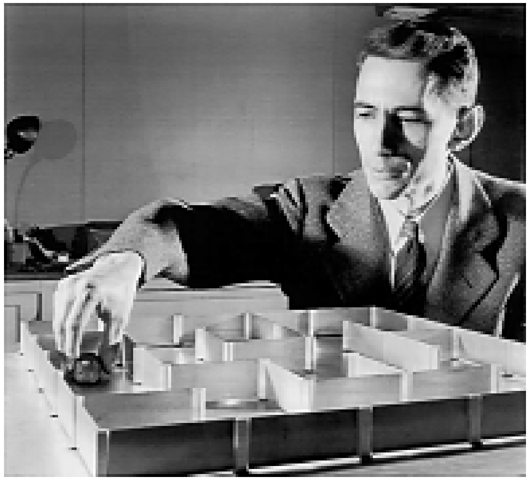
$$\mathcal{E}_\pi(CAB) = \pi(C)\pi(A)\pi(B)$$
$$= Z\ E\ A$$
$$\mathcal{D}_\pi(ZEA) = \pi^{-1}(Z)\pi^{-1}(E)\pi^{-1}(A)$$
$$= C\ A\ B$$

Caesar Cipher

Plain text message	Corresponding cipher text message
Hi Amit, Hope you are doing fine. How about meeting at the train station this Friday at 5 pm? Please let me know if it is ok with you. Regards. Atul	Kl Dplw, Krsh brx duh grlqj ilqh. Krz derxw phhwlqj dw wkh wudlq vwdwlrq wklv Iulgdb dw 5 sp? Sohdvh ohw ph nqrz li lw lv rn zlwk brx. Uhjdugv. Dwxo

Shannon and One-Time Pad Encryption

$$K_e = K_d = \underbrace{K \xleftarrow{\$} \{0,1\}^k}_{\substack{K \text{ chosen at random} \\ \text{from } \{0,1\}^k}}$$



For any $M \in \{0,1\}^k$

- $\mathcal{E}_K(M) = K \oplus M$
- $\mathcal{D}_K(C) = K \oplus C$

Theorem (Shannon): OTP is perfectly secure as long as only one message encrypted.

"Perfect" secrecy, a notion Shannon defines, captures mathematical impossibility of breaking an encryption scheme.

Fact: if $|M| > |K|$, then no scheme is perfectly secure.

Modern Cryptography: Computational Mathematics

Security of a "practical" system must rely not on the impossibility but on the computational difficulty of breaking the system.

("Practical" = more message bits than key bits)

Modern Cryptography: Computational Mathematics

Rather than:

"It is impossible to break the scheme"

We might be able to say:

"No attack using $\leq 2^{160}$ time succeeds with probability $\geq 2^{-20}$"

I.e., Attacks can exist as long as cost to mount them is prohibitive, where Cost = computing time/memory

The Factoring Problem

Input: Composite integer N

Desired output: prime factors of N

Example:

Input: 85

Output: $17, 5$

Can we write a factoring program? Easy!

Alg Factor(N) // N a product of 2 primes

For $i = 2, 3, \ldots, \lceil \sqrt{N} \rceil$ do

If $N \bmod i = 0$ then return i

But this is very slow ...

Can we factor fast?

- Gauss couldn't figure out how
- Nor does anyone know now

Nobody today knows how to factor a 400 digit number in a practical amount of time.

Atomic Primitives or Problems

Examples:

- Factoring: Given large $N = pq$, find p, q
- Block cipher primitives: DES, AES, ...
- Hash functions: MD5, SHA1, ...

New uses for old Mathematics

- Cryptography is based on concepts of
  - Number Theory
  - Combinatorics
  - Modern Algebra
  - Probability Theory

Diffusion and Confusion

- In **Diffusion**, the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having **each plaintext digit affect the value of many ciphertext digits**

- **Confusion** seeks to make the **relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible**.

- **Reference**: "*A Mathematical Theory of Communication*", by Claude Shannon, Bell System Technical Journal, 1948

Permutation & Inverses

A function $f\colon \{0,1\}^\ell \to \{0,1\}^\ell$ is a permutation if there is an inverse function $f^{-1}\colon \{0,1\}^\ell \to \{0,1\}^\ell$ satisfying

$$\forall x \in \{0,1\}^\ell : f^{-1}(f(x)) = x$$

This means f must be one-to-one and onto, meaning for every $y \in \{0,1\}^\ell$ there is a unique $x \in \{0,1\}^\ell$ such that $f(x) = y$.

Permutation & Inverses

x	00	01	10	11
$f(x)$	01	11	00	10

A permutation

x	00	01	10	11
$f(x)$	01	11	11	10

Not a permutation

Permutation & Inverses

x	00	01	10	11
$f(x)$	01	11	00	10

A permutation

x	00	01	10	11
$f^{-1}(x)$	10	00	11	01

Its inverse

Block Ciphers

Let

$$E\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$$

be a function taking a key K and input x to return output $E(K,x)$. For each key K we let $E_K\colon \{0,1\}^\ell \to \{0,1\}^\ell$ be the function defined by

$$E_K(x) = E(K,x)\ .$$

We say that E is a block cipher if

- $E_K\colon \{0,1\}^\ell \to \{0,1\}^\ell$ is a permutation for every K, meaning has an inverse E_K^{-1},
- E, E^{-1} are efficiently computable,

where $E^{-1}(K,x) = E_K^{-1}(x)$.

Block Ciphers: Example

Let $\ell = k$ and define $E\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ by

$$E_K(x) = E(K, x) = K \oplus x$$

Then E_K has inverse E_K^{-1} where

$$E_K^{-1}(y) = K \oplus y$$

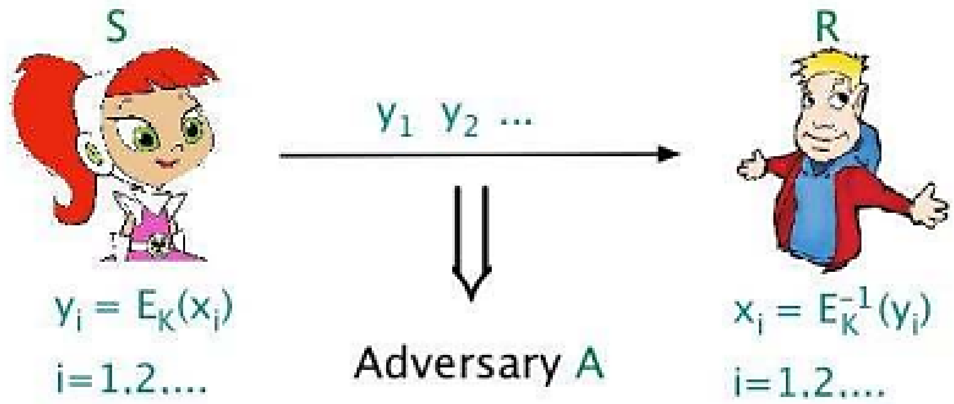
Why? Because

$$E_K^{-1}(E_K(x)) = E_K^{-1}(K \oplus x) = K \oplus K \oplus x = x$$

Block Ciphers: Usage

- $K \leftarrow \{0,1\}^k$
- K (magically) given to parties S, R, but not to A.
- S,R use E_K

Algorithm E is public! Think of E_K as encryption under key K.



Leads to security requirements like:

- Hard to get K from $y_1, y_2, \ldots$
- Hard to get x_i from y_i

Data Encryption Standard (DES)

Key Length $k = 56$

Block length $\ell = 64$

So,

$$\text{DES}\colon \{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$$

$$\text{DES}^{-1}\colon \{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$$

Problem: Already broken!

Advanced Encryption Standard (AES)

1998: NIST announces competition for a new block cipher

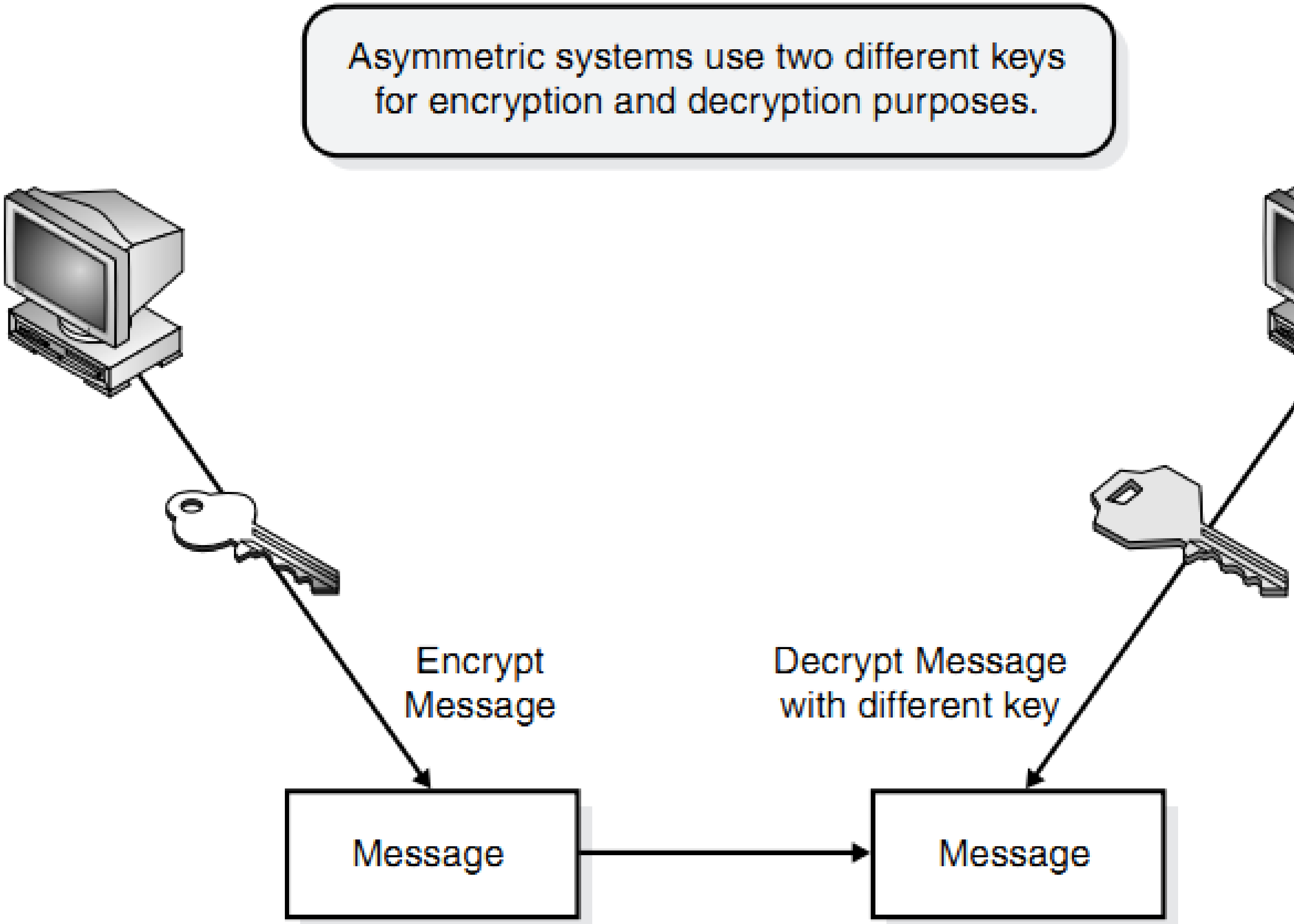
- key length 128
- block length 128
- faster than DES in software

Submissions from all over the world: MARS, Rijndael, Two-Fish, RC6, Serpent, Loki97, Cast-256, Frog, DFC, Magenta, E2, Crypton, HPC, Safer+, Deal

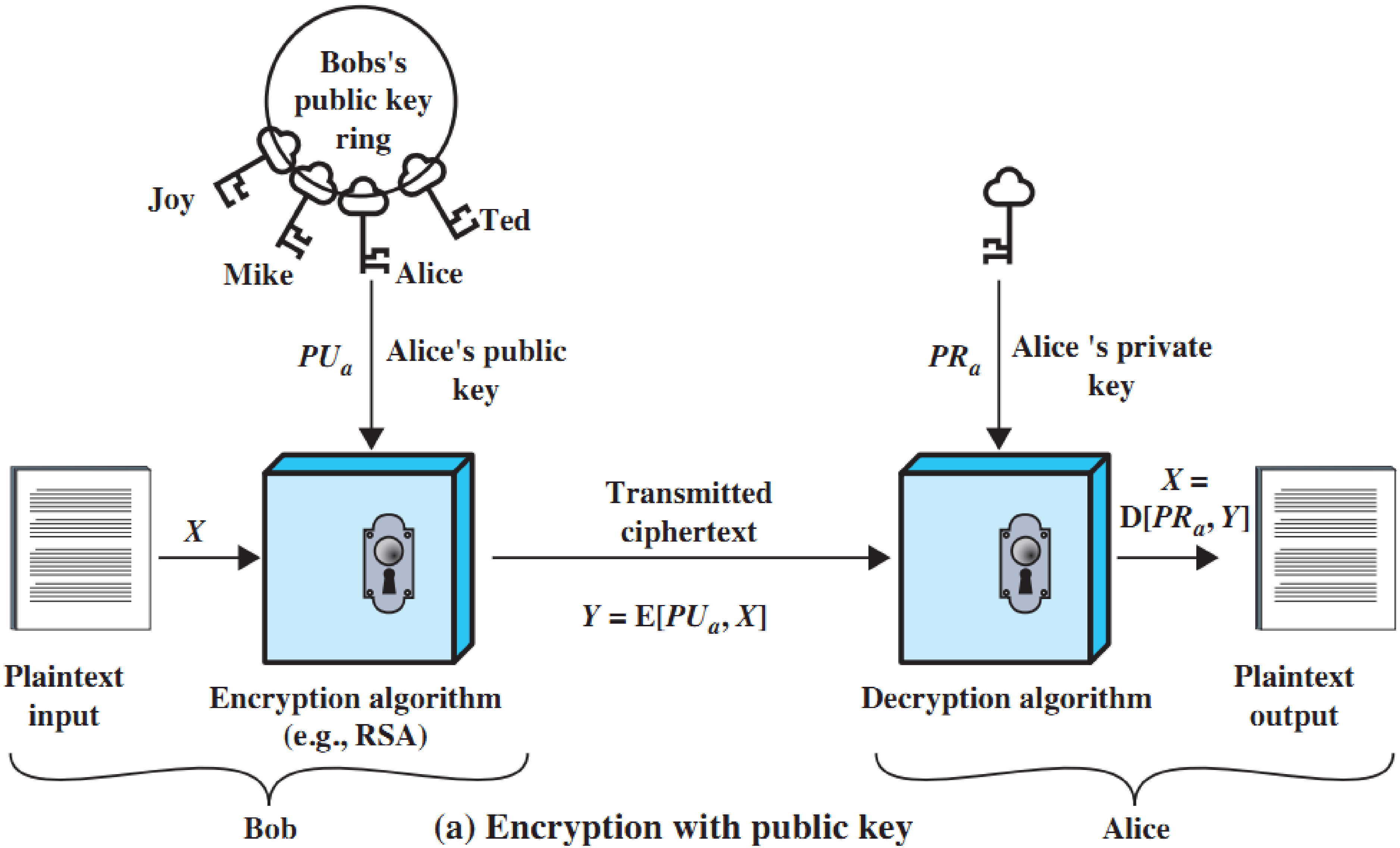
2001: NIST selects Rijndael to be AES.

AES currently dominating **symmetric** encryption method

Public Key / Asymmetric Cryptography

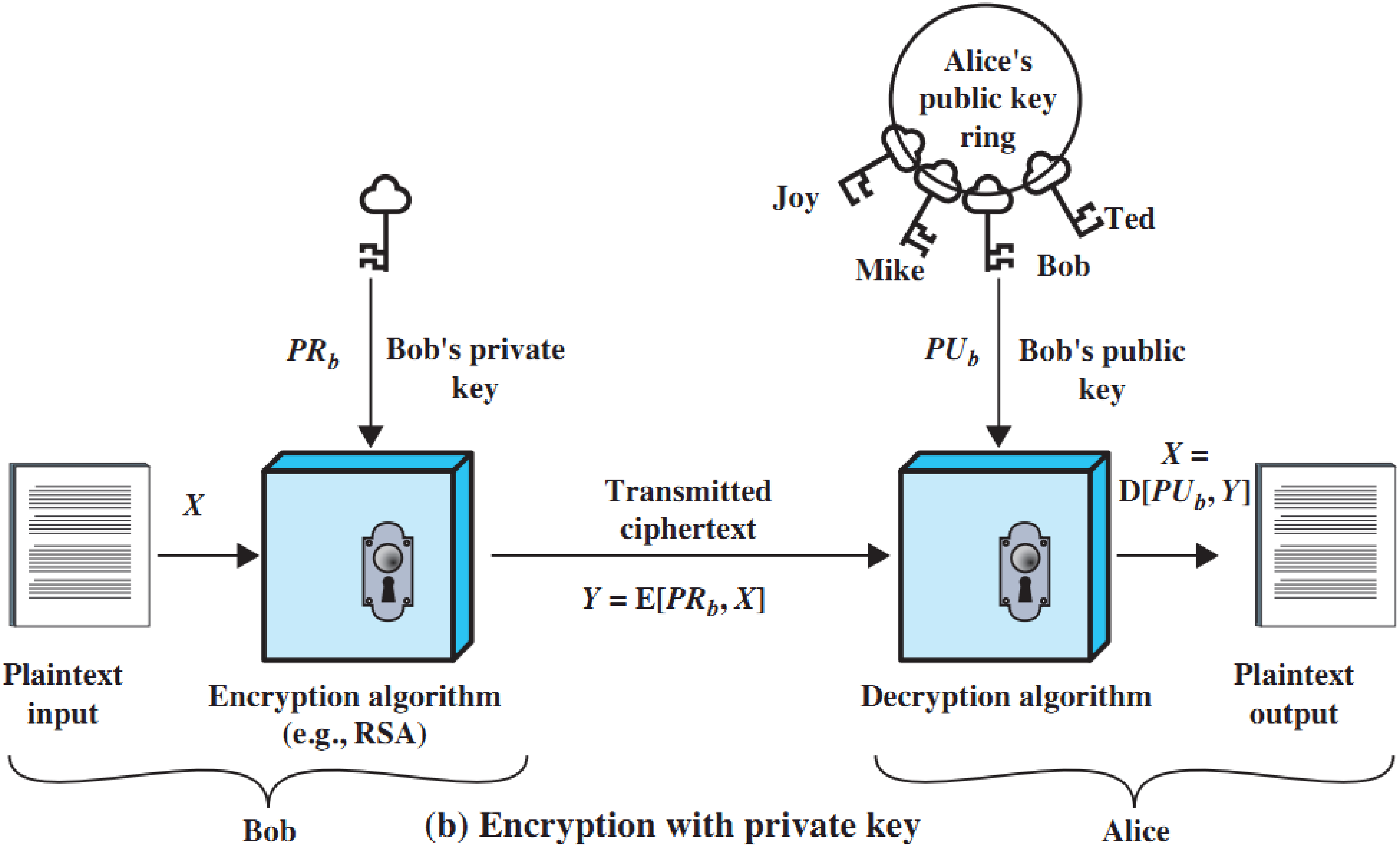


Public Key Cryptography



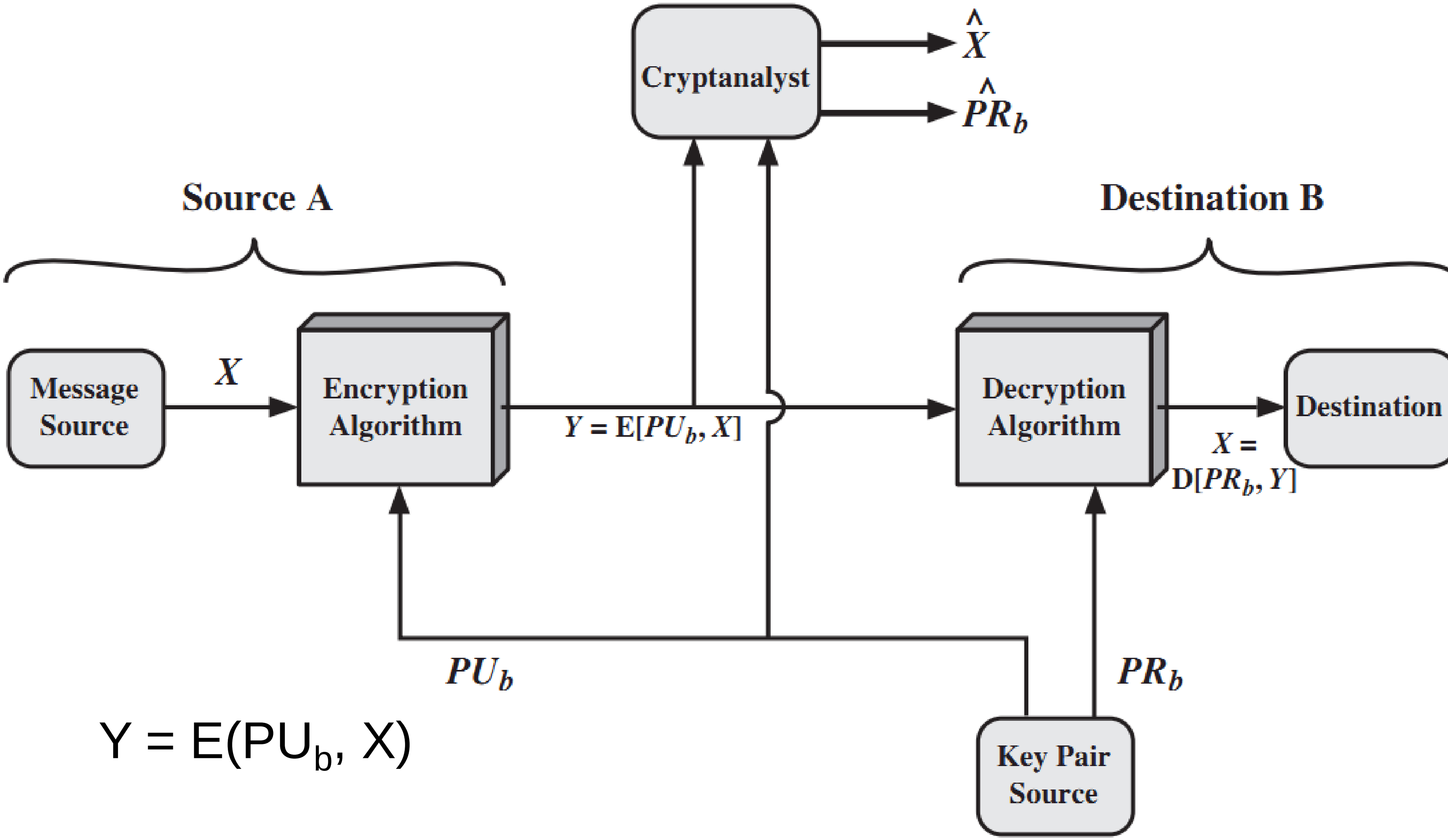
(a) Encryption with public key

Public Key Cryptography



(b) Encryption with private key

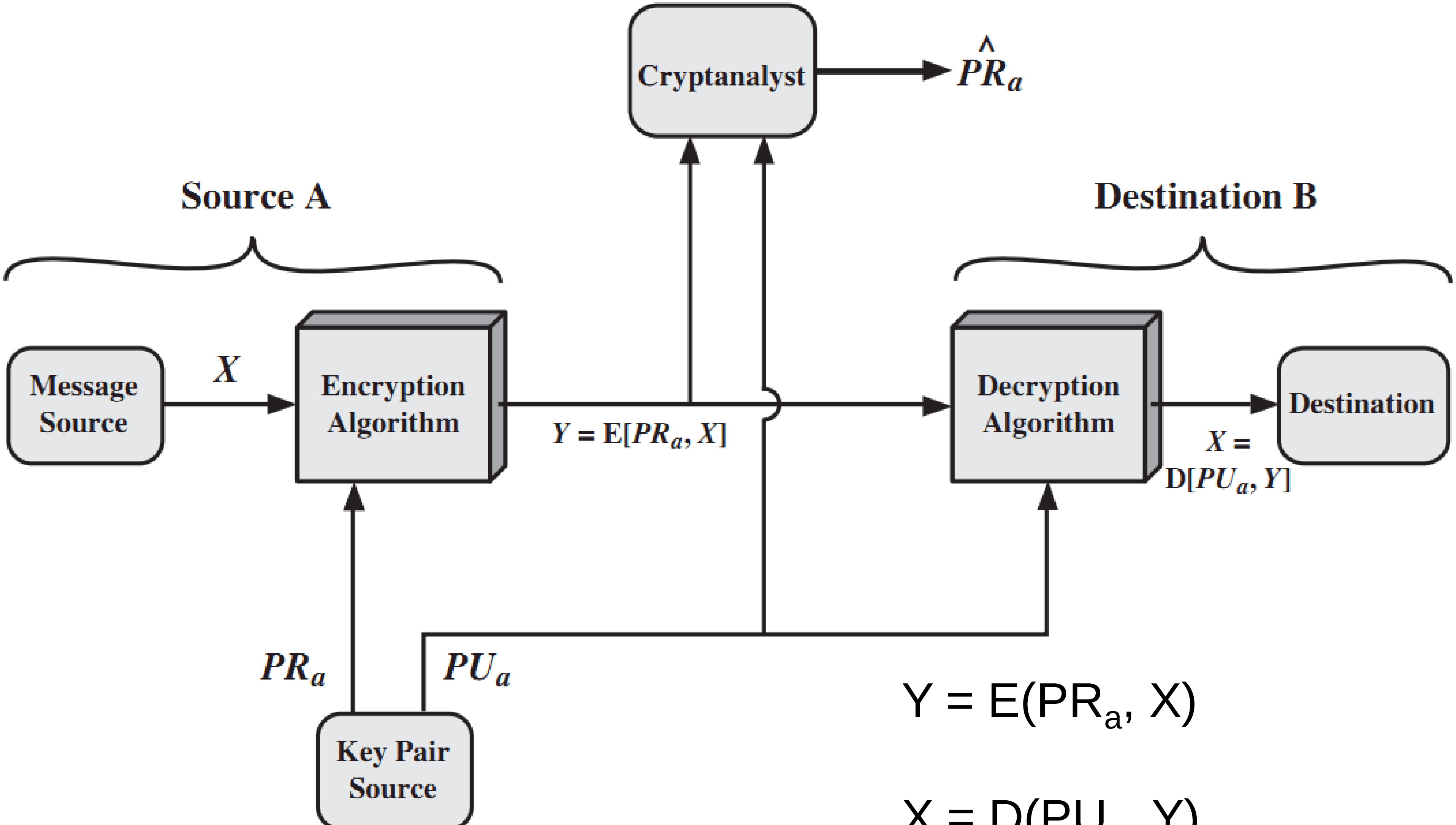
Public Key Cryptography: Secrecy



$Y = E(PU_b, X)$

$X = D(PR_b, Y)$

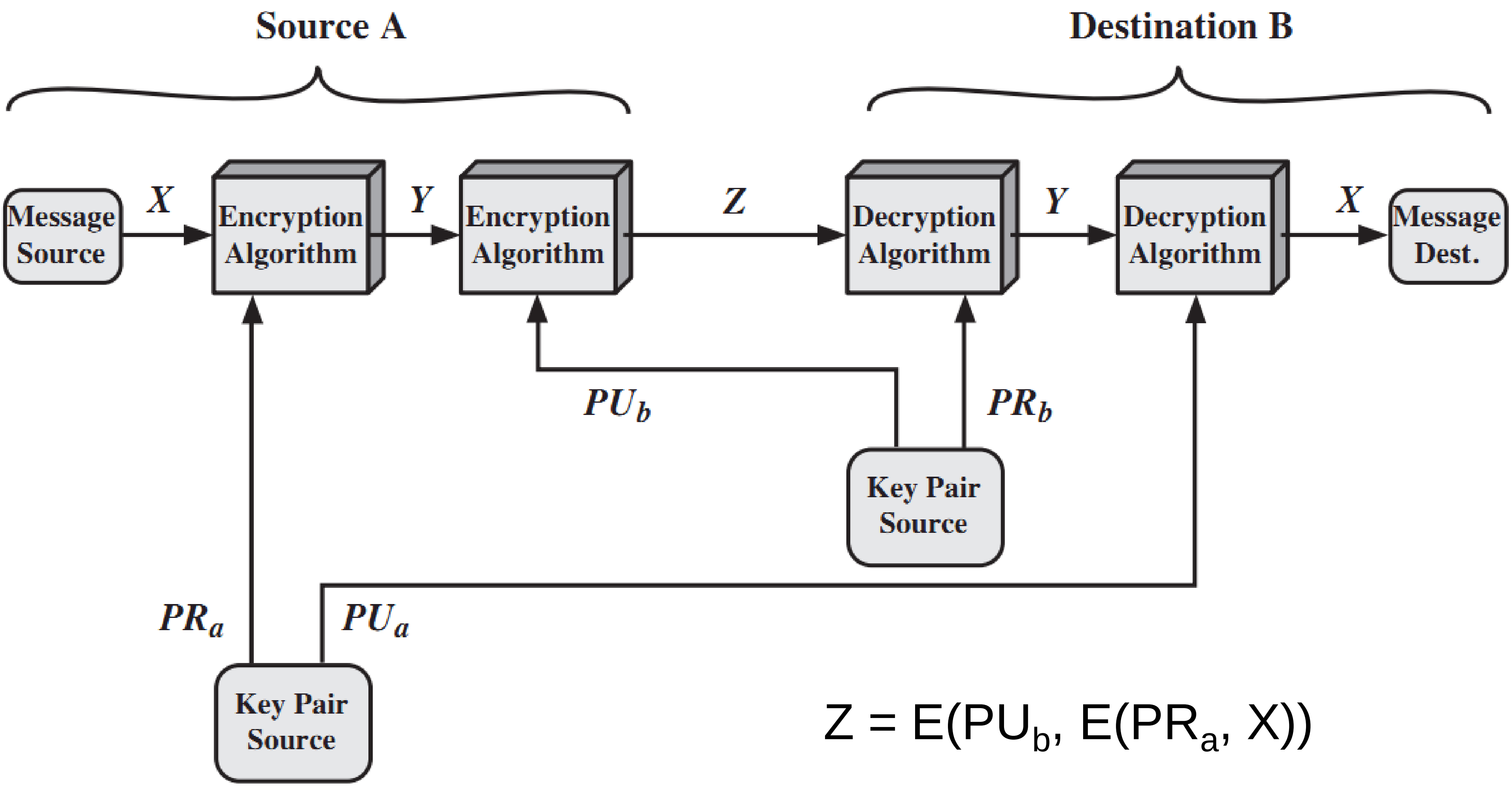
Public Key Cryptography: Authentication



$$Y = E(PR_a, X)$$

$$X = D(PU_a, Y)$$

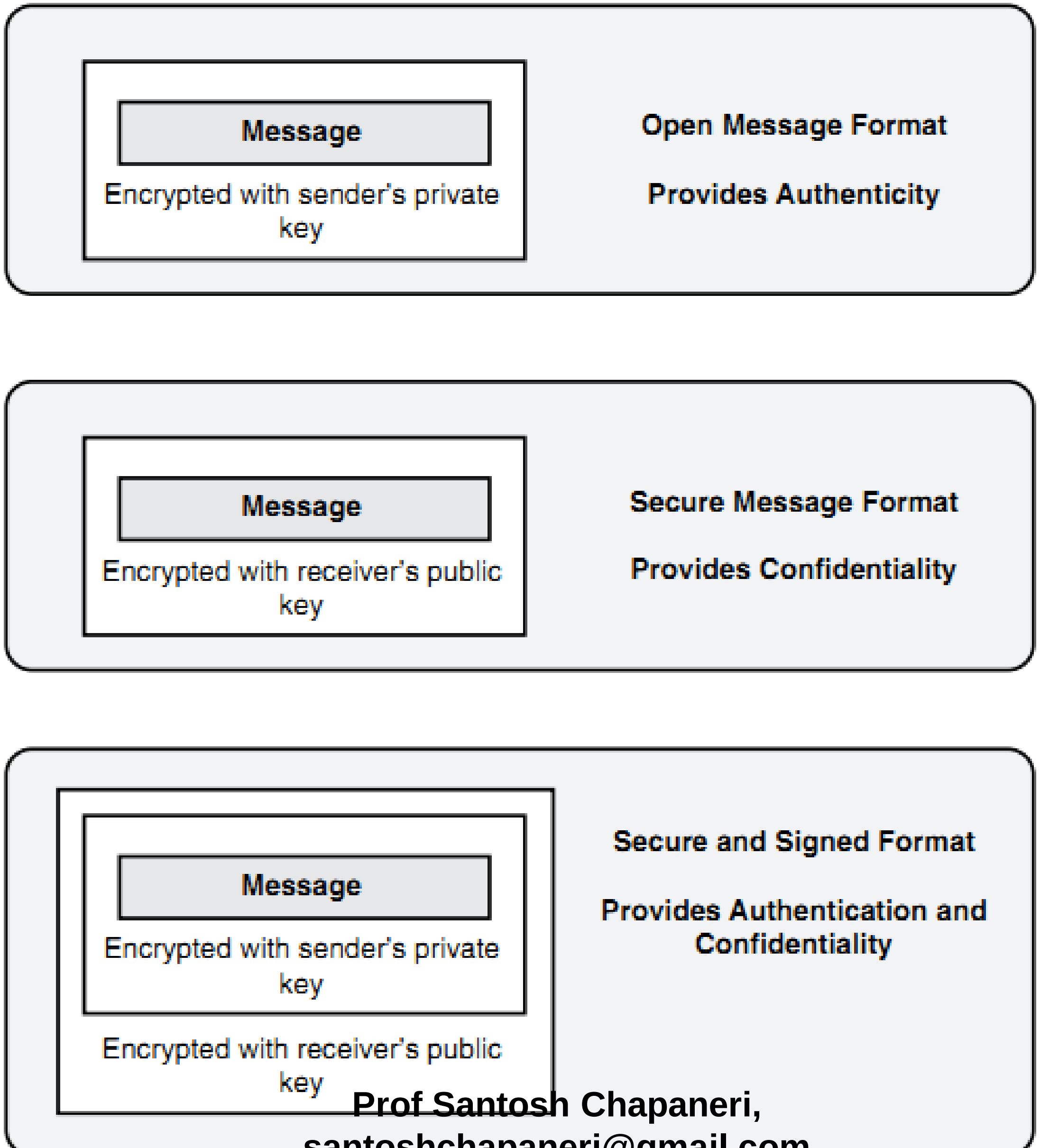
Public Key Cryptography: Secrecy + Authentication



$$Z = E(PU_b, E(PR_a, X))$$

$$X = D(PU_a, D(PR_b, Z))$$

Public Key Cryptography



One-Way Trapdoor Function

- A ***one-way function*** is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy whereas the calculation of the inverse is infeasible: **$Y = f(X)$ easy but $X = f^{-1}(Y)$ infeasible**

- For example, if the length of the input is n bits and the time to compute the function is proportional to 2^n (**exponential time**), the problem is considered **infeasible**.

- **Trapdoor one-way function** means easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known.

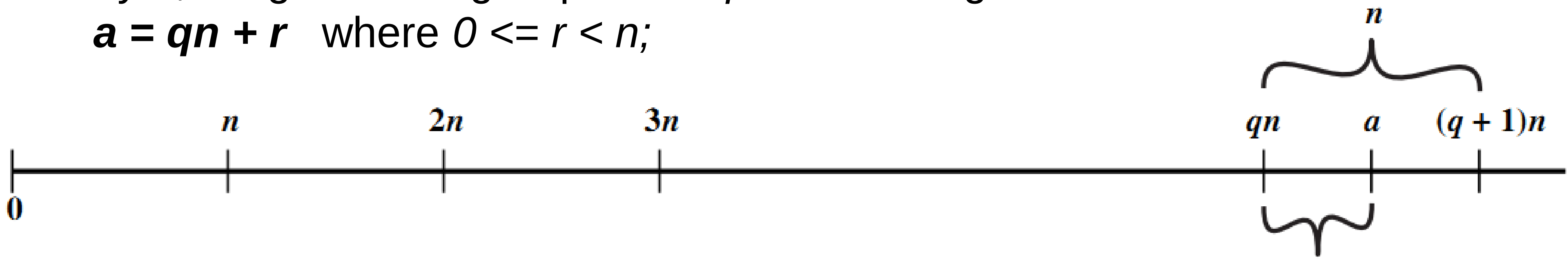
- A trap-door one-way function means:
  - $Y = f_k(X)$ easy, if k and X are known
  - $X = f_k^{-1}(Y)$ easy, if k and Y are known
  - $X = f_k^{-1}(Y)$ infeasible, if Y known but k not known

One-Way Trapdoor Function

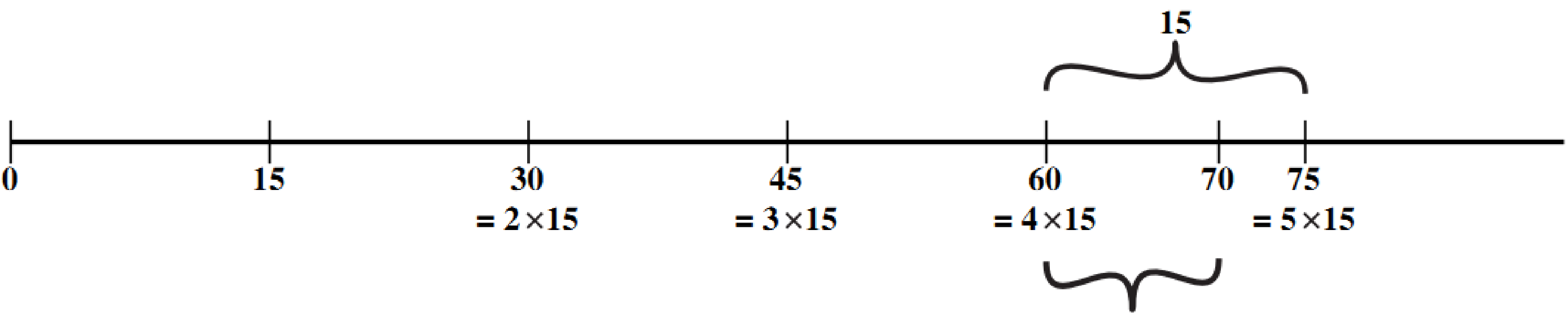
- Example: Consider primes p = 48611 and q = 53993, so $n = pq$ = 2624653723
- If only n is known, but p and q are not known, then prime factorization is a non-trivial computationally inefficient problem.
- Selecting p and q to be distinct prime numbers (each 100 decimal digits), then factoring $n = pq$ is a difficult problem even by today's standards.

Modular Arithmetic

- Given any positive integer *n* and any nonnegative integer *a*, if we divide *a* by *n*, we get an integer quotient *q* and an integer remainder *r* such that:
  a* = *qn* + *r   where $0 <= r < n$;



(a) General relationship



(b) Example: 70 = (4×15) + 10

- If *a* is an integer and *n* is a positive integer, we define ***a* mod *n*** to be the **remainder r when *a* is divided by *n***.

Modular Arithmetic

- Two integers *a* and *b* are said to be **congruent modulo** *n*, if (*a* mod *n*) = (*b* mod *n*). This is written as

$$a \equiv b \pmod{n}$$

- Eg: $73 \equiv 4 \pmod{23}$; $21 \equiv -9 \pmod{10}$;
  $23 \equiv 8 \pmod{5}$; $81 \equiv 0 \pmod{27}$

- **Exponentiation** is performed by repeated multiplication, as in ordinary arithmetic. To find 11^7 mod 13:
- **11^2** = 121 ≡ 4 mod 13, **11^4** ≡ 4^2 ≡ 3 mod 13, so **11^7** = 11 x 11^4 x 11^2 ≡ 11 x 3 x 4 ≡ 132 ≡ 2 mod 13.

Fermat's Theorem

- **Fermat's Theorem**:

  $a^{p-1} \equiv 1 \pmod{p}$, where p is prime and gcd(a, p) = 1

- Example of Fermat's Theorem: a = 7, p = 19
- 7^2 = 49 ≡ 11 mod 19,
- 7^4 ≡ 121 ≡ 7 mod 19,
- 7^8 ≡ 49 ≡ 11 mod 19,
- 7^16 ≡ 121 ≡ 7 mod 19, so
- 7^18 = 7^16 x 7^2 ≡ 7 x 11 = 77 ≡ 1 mod 19

Euler's Theorem

- **Euler's Totient Function** Φ(n): defined as the number of positive integers less than n and relatively prime to n. By definition, Φ(1) = 1

- Determine Φ(37) and Φ(35)
- Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus Φ(37) = 36.
- To determine Φ(35), we list all of the positive integers less than 35 that are relatively prime to it: 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34. There are 24 numbers on the list, so Φ(35) = 24.

- **For a prime number p, Φ(p) = p – 1** => For **n = pq, Φ(n) = Φ(p) x Φ(q) if p and q are prime**.

  Φ(21) = Φ(3) x Φ(7) = 2 x 6 = 12

Inverse Modulo

- **Euler's Theorem**: **For every a and n that are relatively prime**, $\mathbf{a^{\Phi(n)} \equiv 1 \bmod n}$
- Example: a = 3, n = 10

  $\Phi(10) = 4$, $3^4 = 81 \equiv 1 \bmod 10$
- Example: a = 2, n = 11

  $\Phi(11) = 10$, $2^{10} = 1024 \equiv 1 \bmod 11$

- How to find **Inverse Modulo**: $\mathbf{a^{-1} \bmod n = a^{\Phi(n)\,-1} \bmod n}$
- Example: $70^{-1} \bmod 3$

  $70^{\Phi(3)-1} \bmod 3 = 70^{2-1} \bmod 3 = 70^{1} \bmod 3 = 1$

RSA Algorithm

Key Generation by Alice

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key

Plaintext: $M < n$

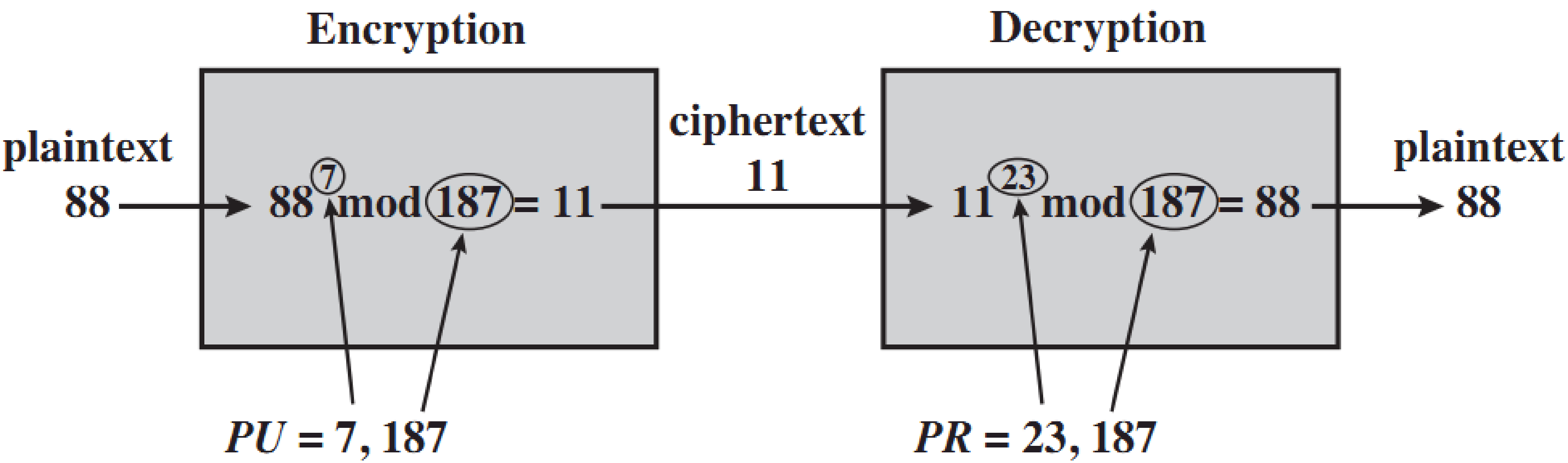
Ciphertext: $C = M^e \bmod n$

Decryption by Alice with Alice's Private Key

Ciphertext: C

Plaintext: $M = C^d \bmod n$

RSA Example



p =17, q = 11, so Φ(n) = 16 x 10 = 160, choose e = 7, de ≡ 1 mod 160, d = 23 (23x7=161)

For **encryption**, we need to calculate C = 88^7 mod 187

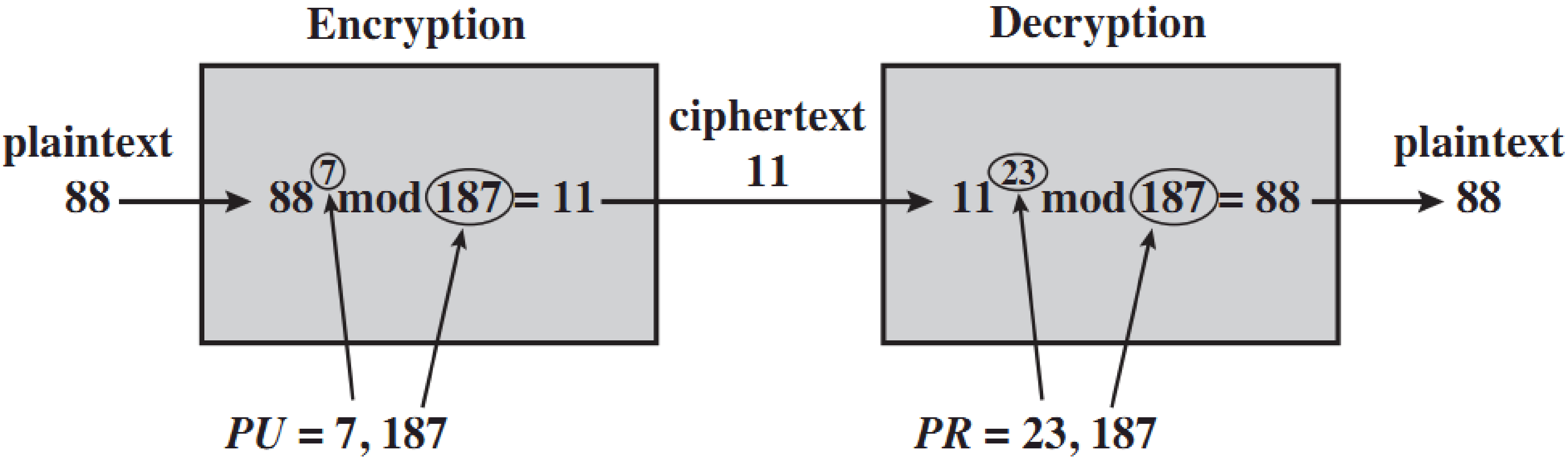
88^7 mod 187 = [(88^4 mod 187) x (88^2 mod 187) x (88^1 mod 187)] mod 187

88^2 mod 187 = 7744 mod 187 = 77

88^4 mod 187 = 59,969,536 mod 187 = 132

88^7 mod 187 = (88 x 77 x 132) mod 187 = 894,432 mod 187 = 11

RSA Example



For **decryption**, we calculate M = 11^{23} mod 187

11^{23} mod 187 = [(11^1 mod 187) x (11^2 mod 187) x (11^4 mod 187) x (11^8 mod 187) x (11^8 mod 187)] mod 187

11^2 mod 187 = 121

11^4 mod 187 = 14,641 mod 187 = 55

11^8 mod 187 = 214,358,881 mod 187 = 33

11^{23} mod 187 = (11 x 121 x 55 x 33 x 33) mod 187 = 79,720,245 mod 187 = 88

RSA: Selection of *p* and *q*

- The prime numbers p and q should be selected such that the **factoring of n = pq is computationally infeasible**. Both p and q should be of the same bit length and sufficiently large.

- The prime numbers p and q should be such that the difference between p and q should not be very small.

➢ If p-q is small, then p ≈ q. Hence p ≈ sqrt(n). Thus, n could be factored by brute-force attack.

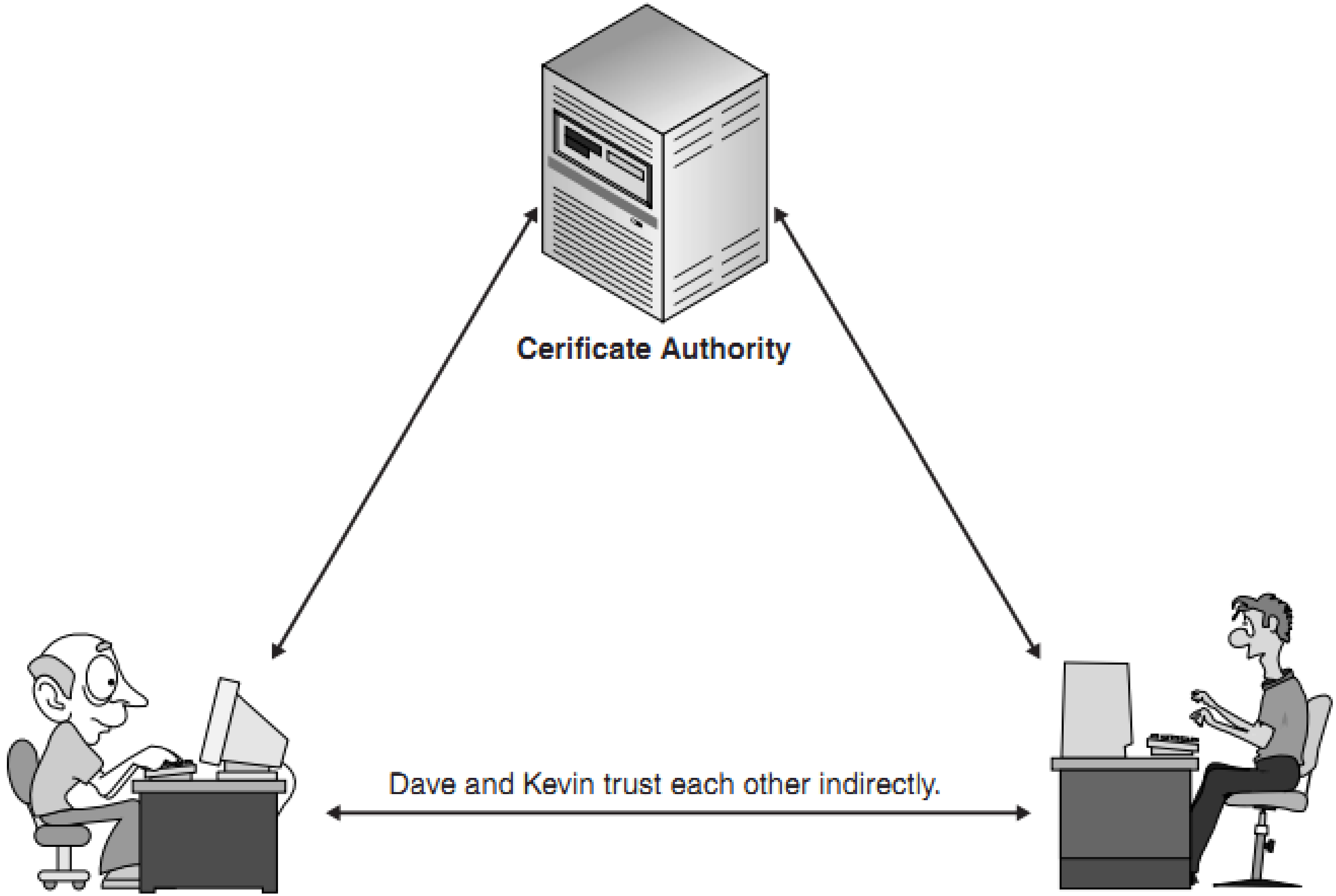
Why is RSA secure?

Only the corresponding Private Key will know how to open the one-way function trap door.

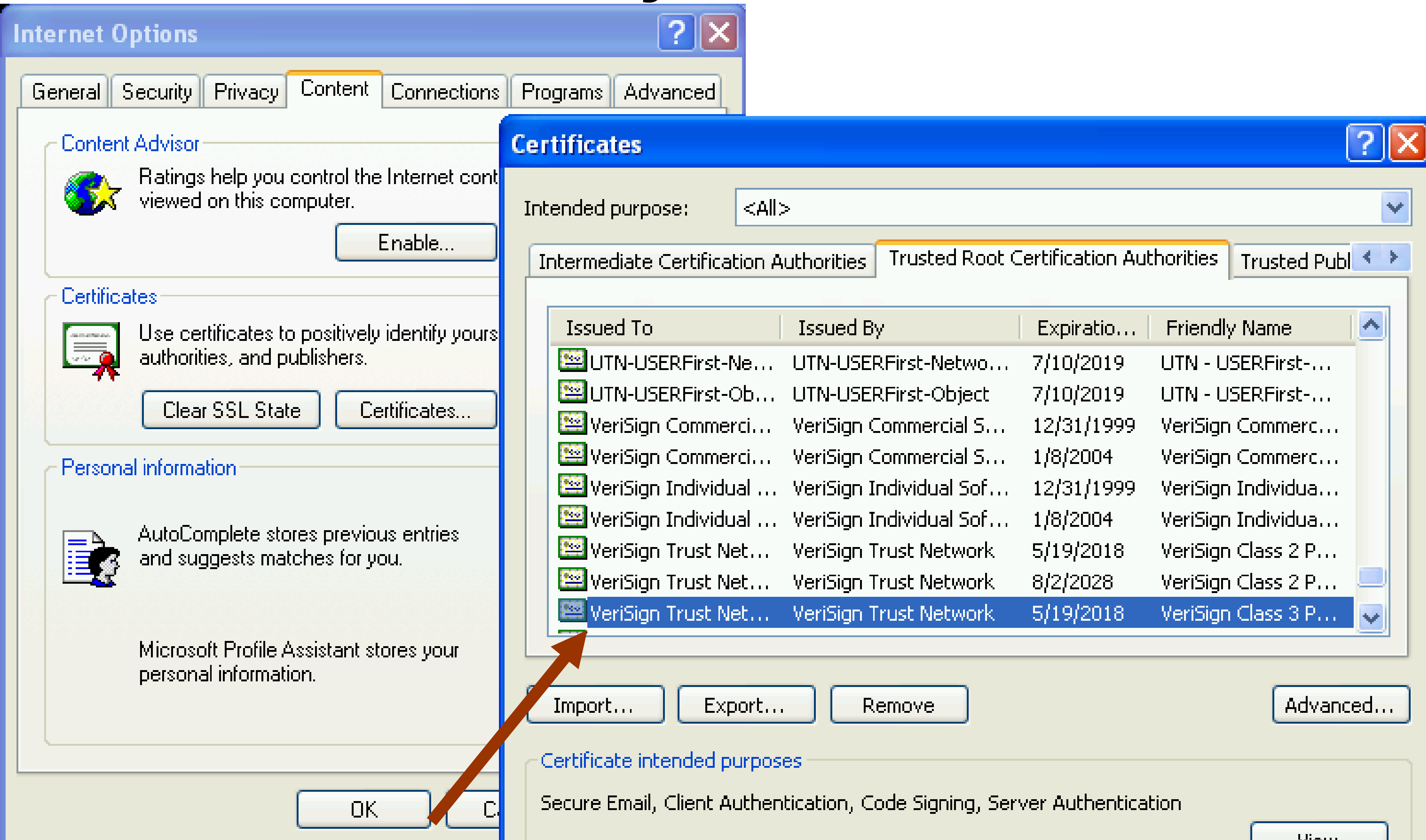
Because only the private key knows how to open the trapdoor, it provides a high level of protection.

One-way Function Trap Door

Certificate Authority (public keys)

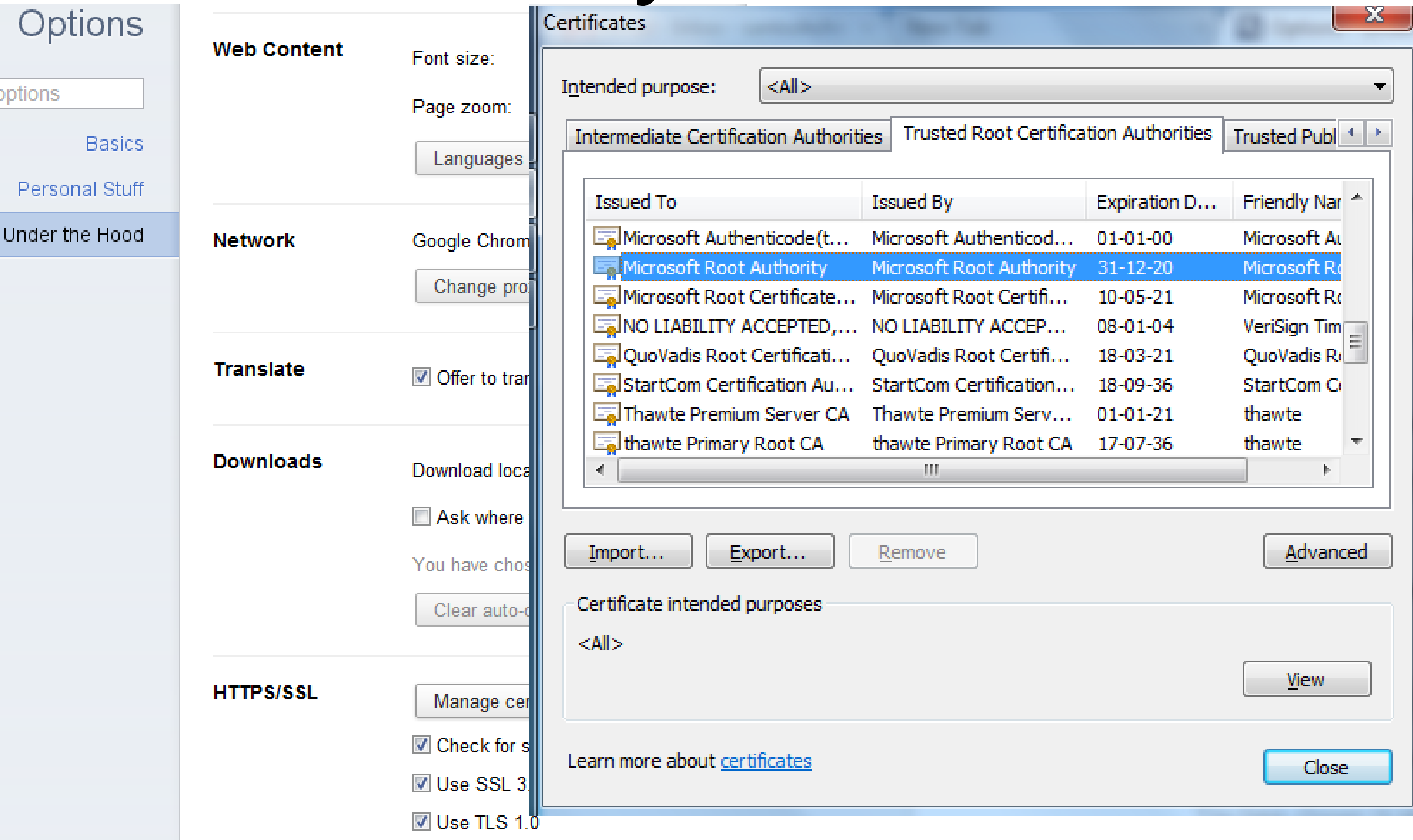


Public Key Certificates

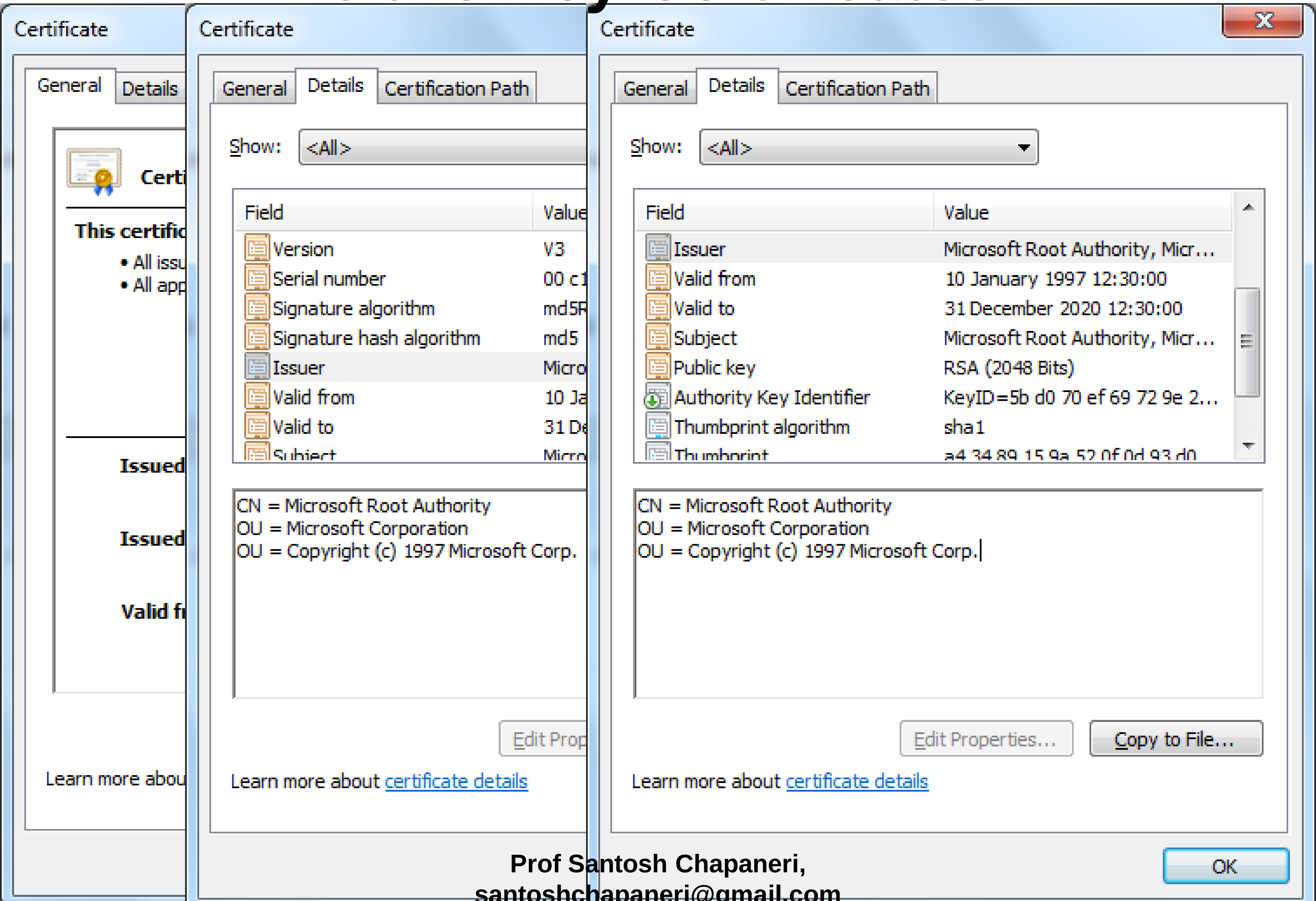


Public Key: (RSA 1024-bit) 30 81 89 02 81 81 00 cc 5e d1 11 5d 5c 69 d0 ab d3 b9 6a 4c 99 1f 59 98 30 8e 16 85 20 46 6d 47 3f d4 85 20 84 e1 6d b3 f8 a4 ed 0c f1 17 0f 3b f9 a7 f9 25 d7 c1 cf 84 63 f2 7c 63 cf a2 47 f2 c6 5b 33 8e 64 40 04 68 c1 80 b9 64 1c 45 77 c7 d8 6e f5 95 29 3c 50 e8 34 d7 78 1f a8 ba 6d 43 91 95 8f 45 57 5e 7e c5 fb ca a4 04 eb ea 97 37 54 30 6f bb 01 47 32 33 cd dc 57 9b 64 69 61 f8 9b 1d 1c 89 4f 5c 67 02 03 01 00 01

Public Key Certificates

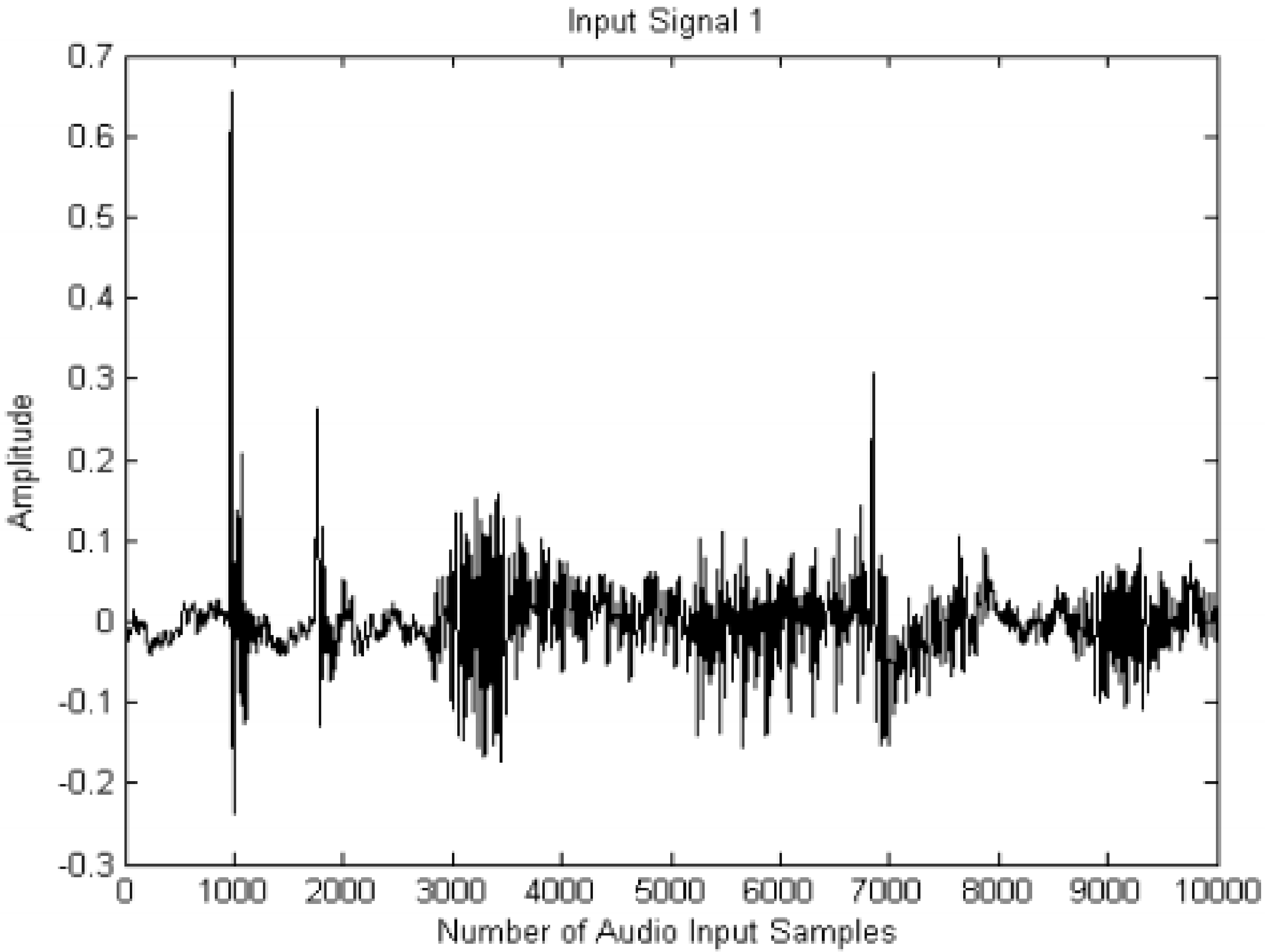


Public Key Certificates



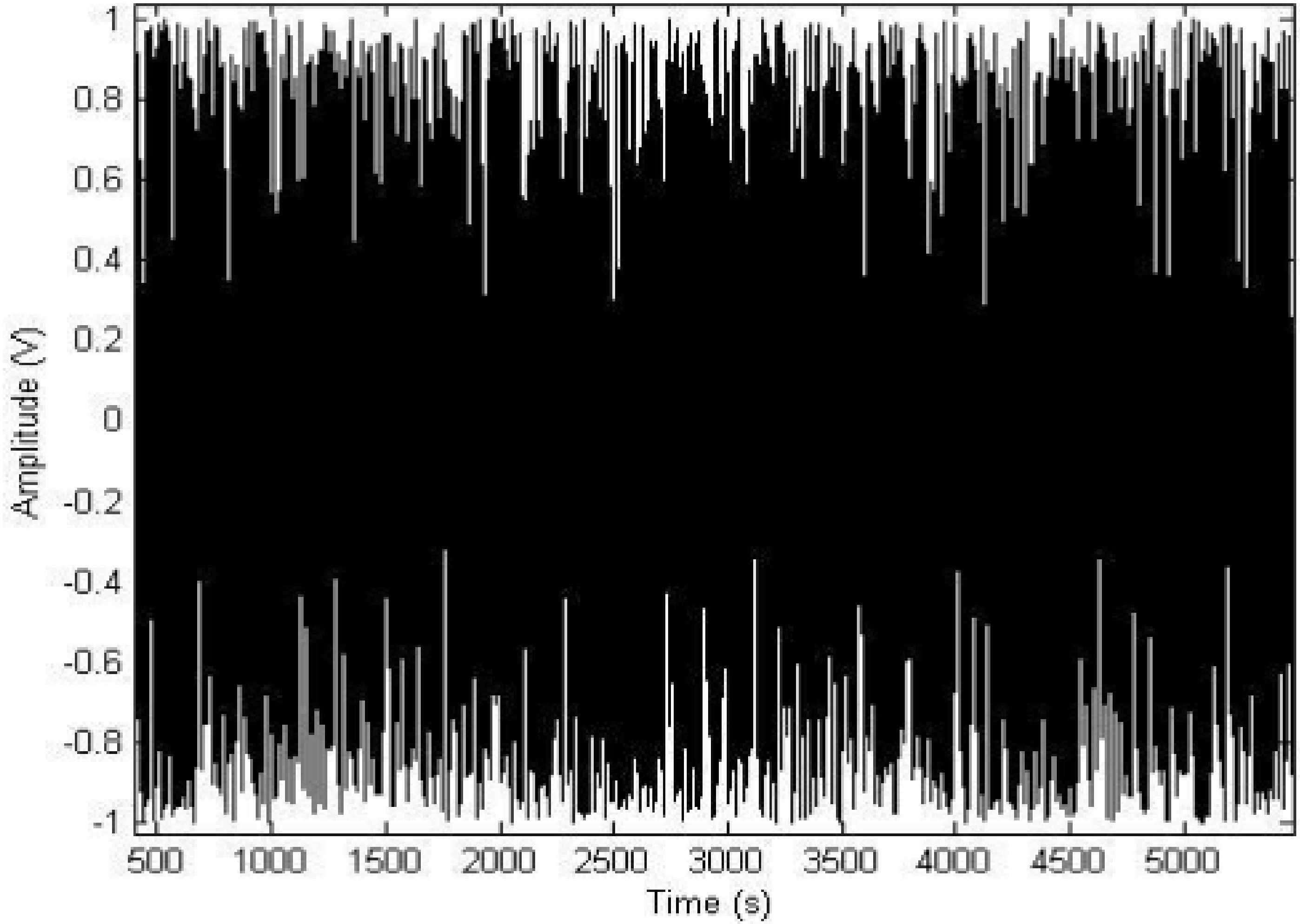
Some applications of Cryptography

Audio Encryption



Original Signal as a function of time

Audio Encryption



Encrypted Signal as a function of time

Image Encryption

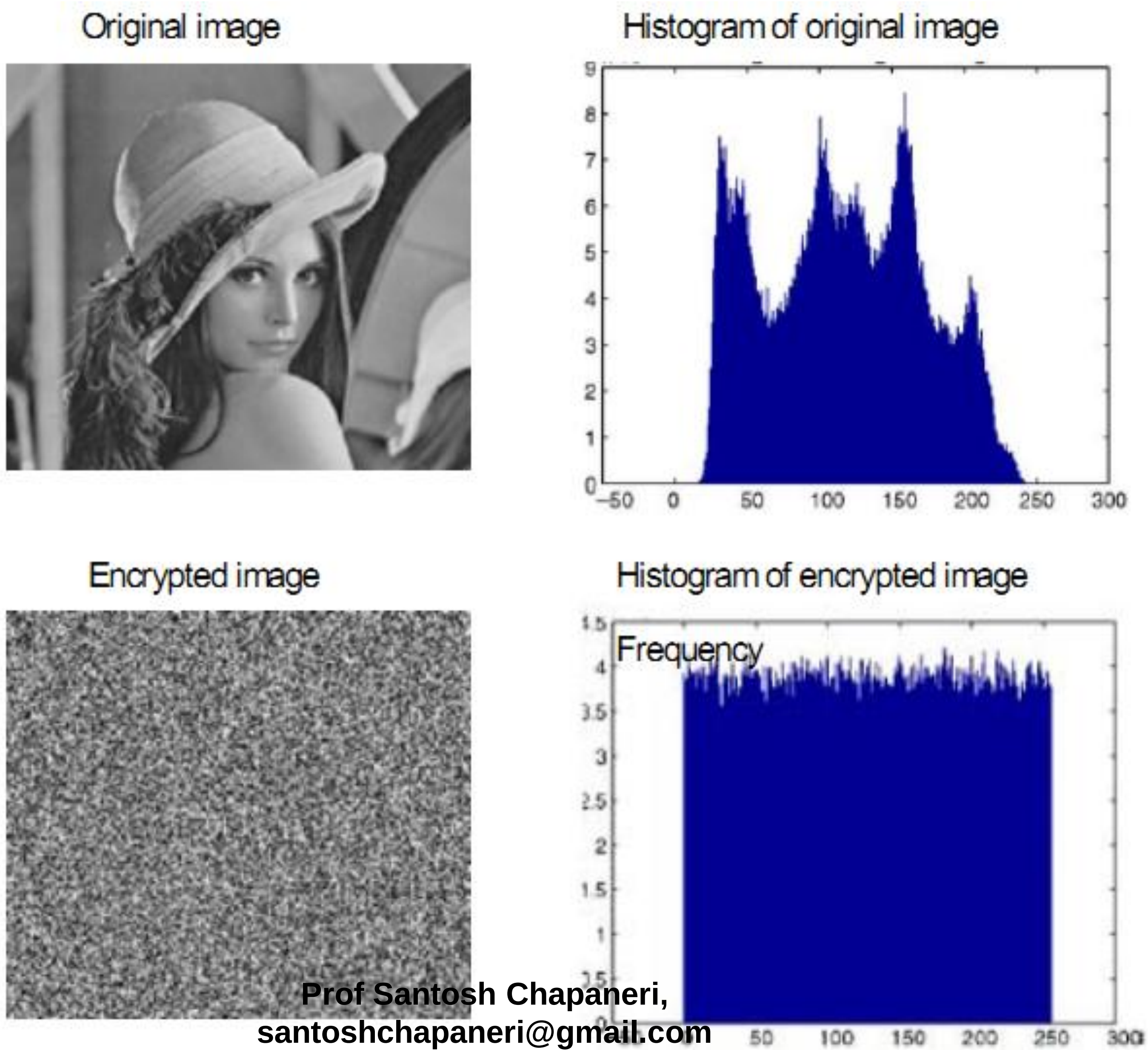
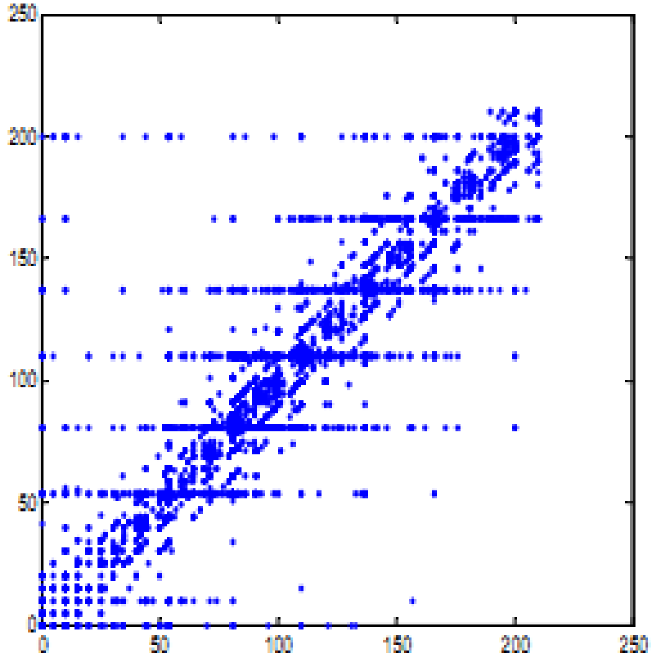
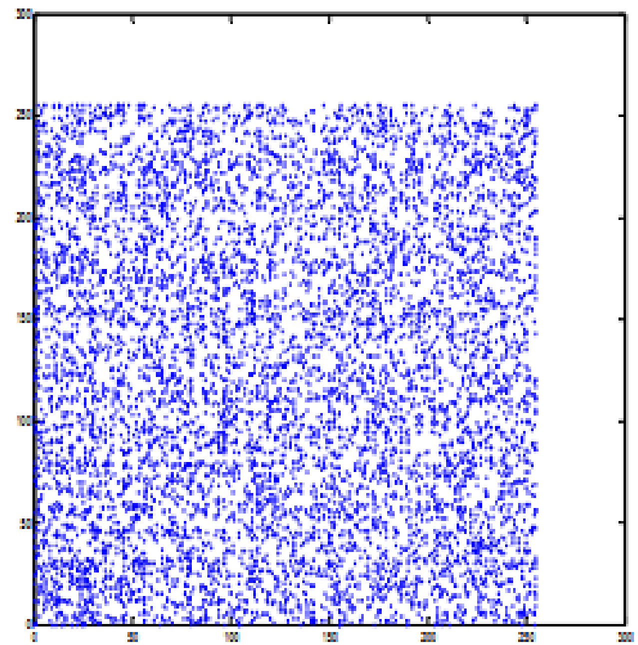


Image Encryption





(a) (b)

Correlation of two horizontally adjacent pixels

(a) in the plain-image, and

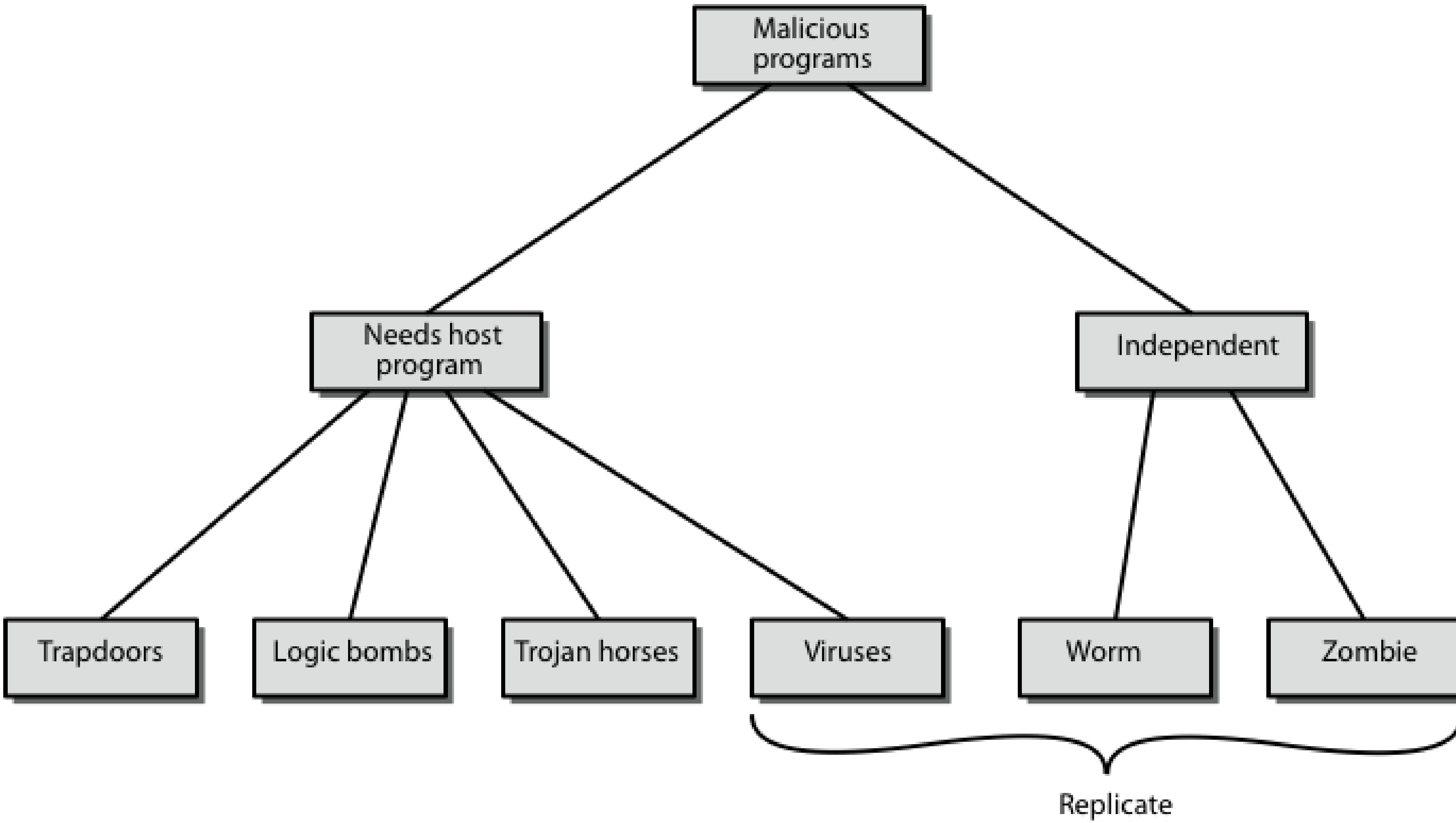
(b) in the ciphered-image

Video Encryption

Regular MPEG-2 video (AKIYO Frame#101)

Encrypted (AKIYO Frame#101) with fixed 256-bit AES

Security: Malicious Programs

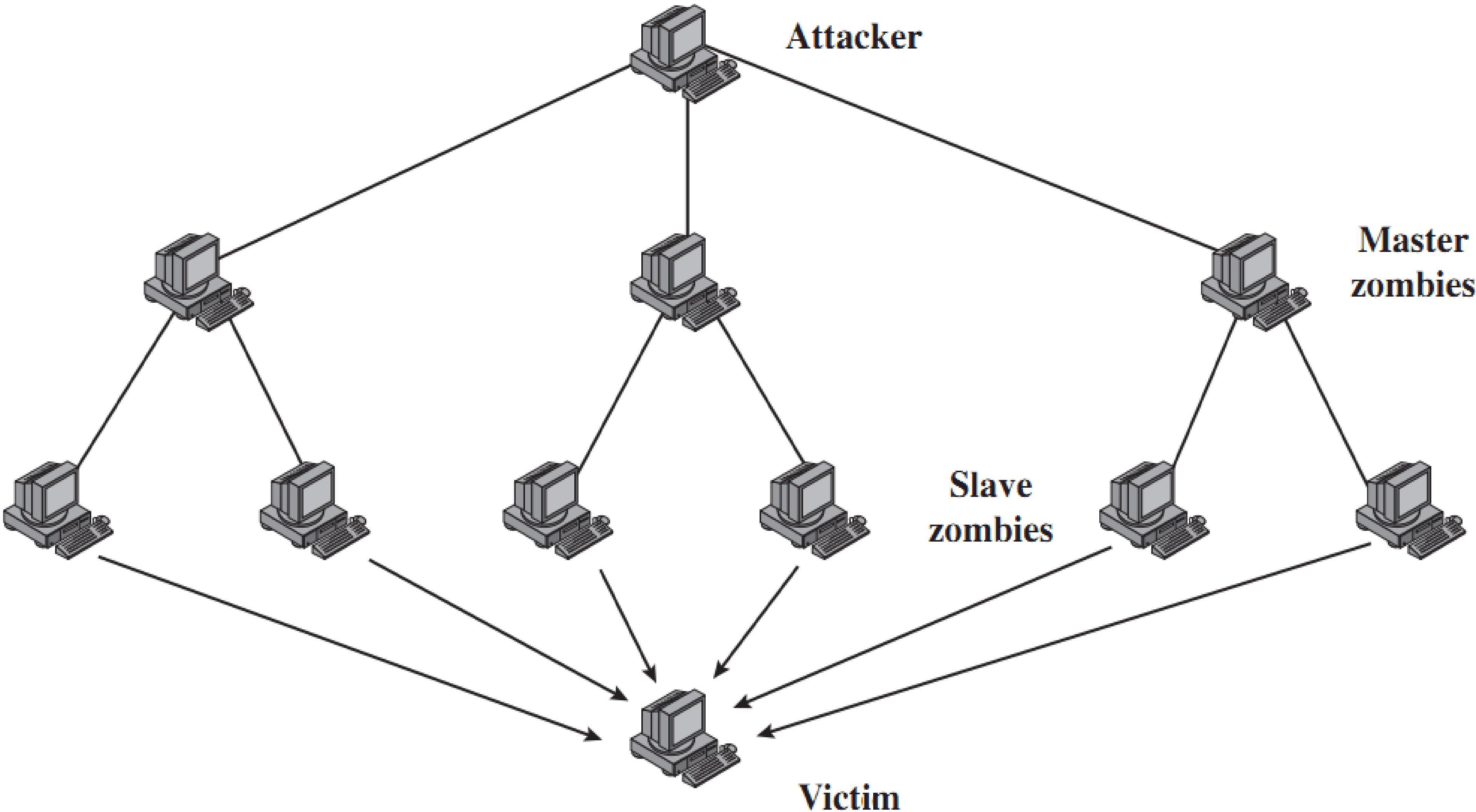


Prof Santosh Chapaneri,
santoshchapaneri@gmail.com

Security: Malicious Programs

Virus	Resides in an executable file and propagates to other executables
Logic bomb	A virus whose payload is delayed and is triggered by some event in the computer
Time bomb	A special case of a logic bomb where the trigger is a particular time or date
Backdoor	A hidden feature in software (normally Trojan or spyware) that gives certain people special privileges denied to others
Worm	Executes independently of other programs, replicates itself, and spreads through a network
Trojan horse	Hides in the computer as an independent program and has a malicious function

Denial of Service Attack

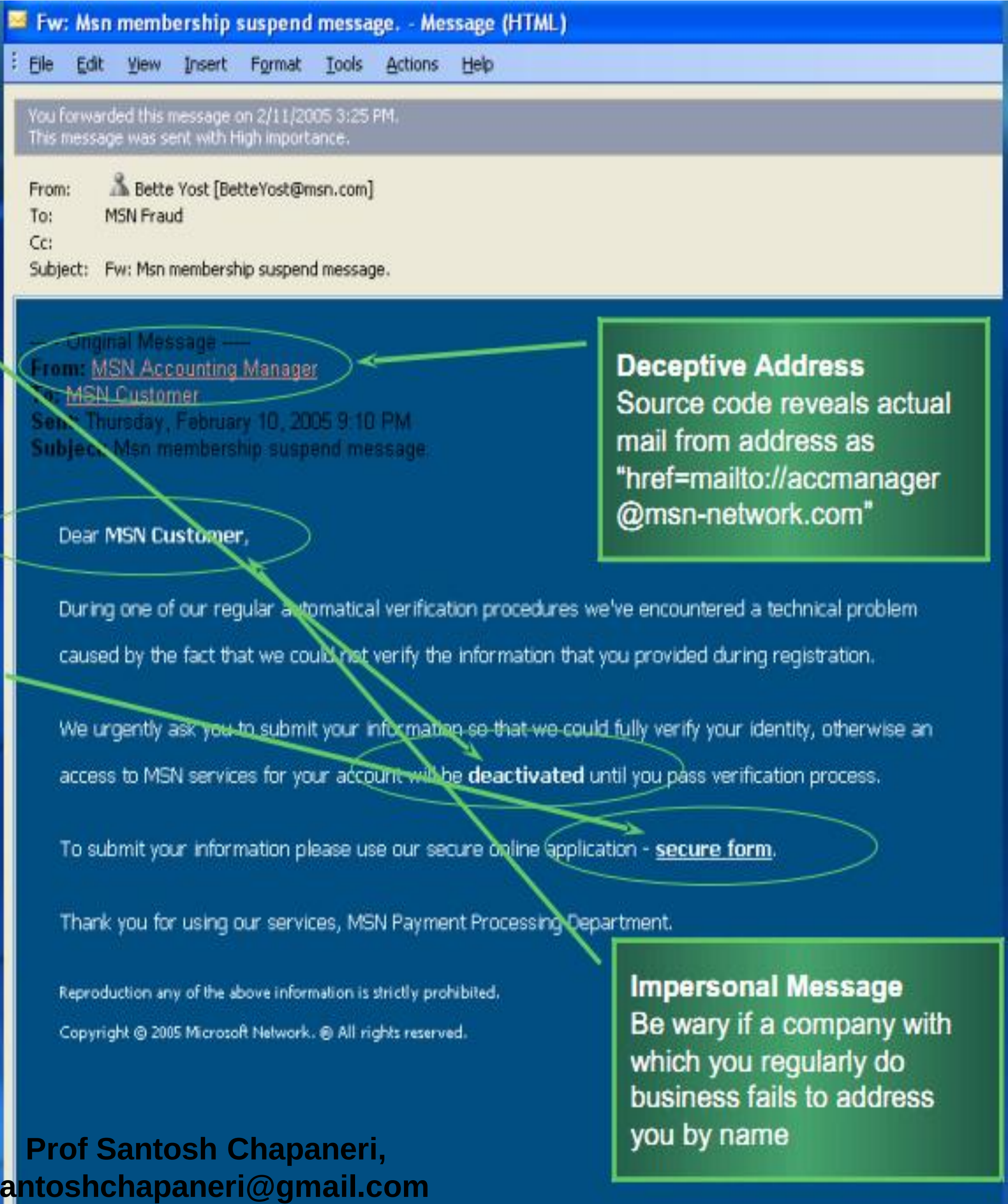


Phishing

Alarmist Message
Criminals try their best to create a sense of urgency so you'll respond without thinking. Also, look for misspellings, grammatical errors, and typos--such as "...an access to MSN services for your account..."

Deceptive Link
Source code reveals that the actual address linked to is "href=http://www.online-msnupdate.com/?sess=qCKWmHUBPPZwT8n4GEMNn70wHDEG140IHKG5tAGiqGOINeov&amp:cid=bettevost@msn.com"

The difference between these two URLs could be a sign that the message is fake. (However, even if the URLs are the same, don't let down your guard, because the pop-up could be a trick, too.)


Fw: Msn membership suspend message. - Message (HTML)

File Edit View Insert Format Tools Actions Help

You forwarded this message on 2/11/2005 3:25 PM.
This message was sent with High importance.

From: Bette Yost [BetteYost@msn.com]
To: MSN Fraud
Cc:
Subject: Fw: Msn membership suspend message.

----- Original Message -----
From: MSN Accounting Manager
To: MSN Customer
Sent: Thursday, February 10, 2005 9:10 PM
Subject: Msn membership suspend message.

Dear **MSN Customer**,

During one of our regular automatical verification procedures we've encountered a technical problem caused by the fact that we could not verify the information that you provided during registration.

We urgently ask you to submit your information so that we could fully verify your identity, otherwise an access to MSN services for your account will be **deactivated** until you pass verification process.

To submit your information please use our secure online application - secure form.

Thank you for using our services, MSN Payment Processing Department.

Reproduction any of the above information is strictly prohibited.

Copyright © 2005 Microsoft Network. ® All rights reserved.

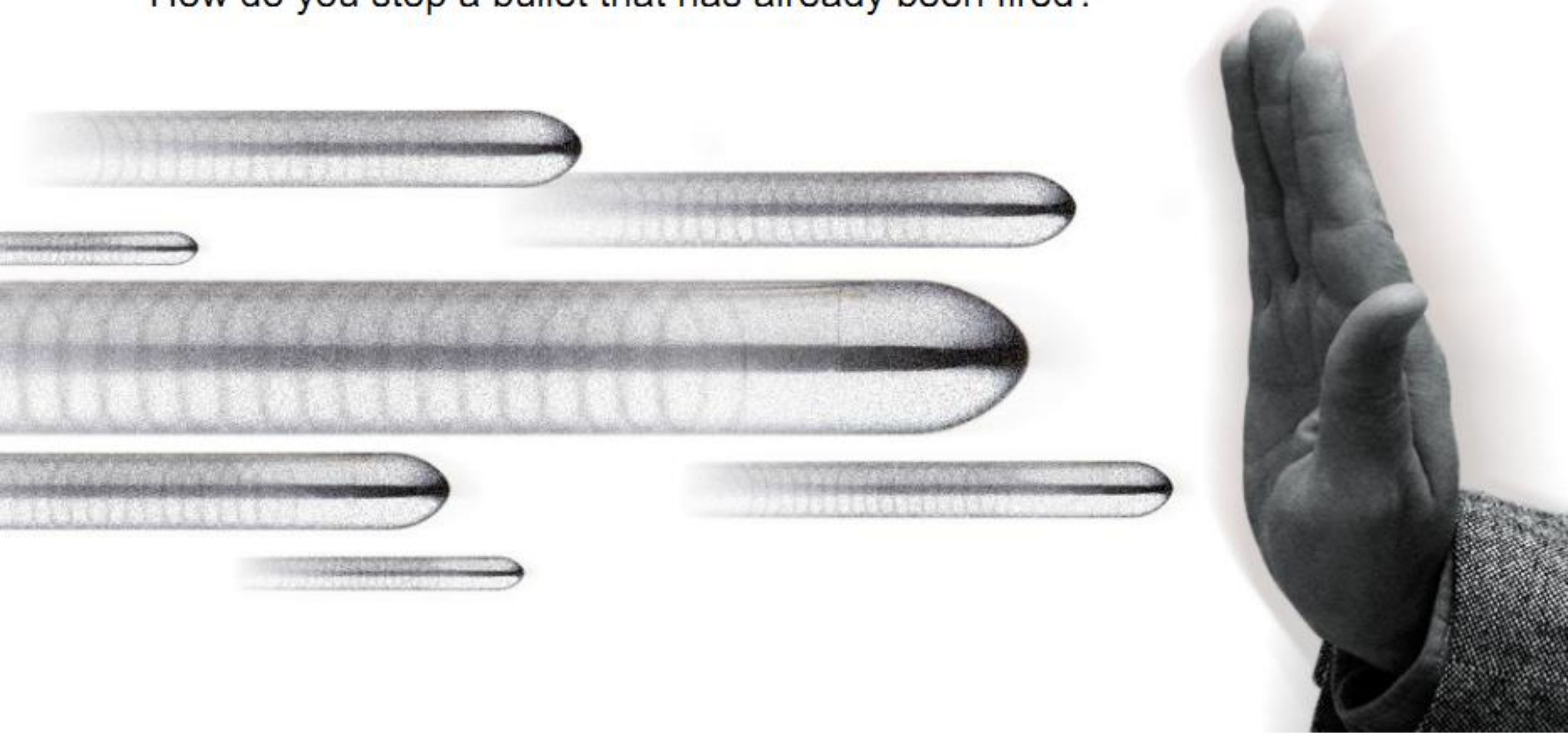
Deceptive Address
Source code reveals actual mail from address as "href=mailto://accmanager@msn-network.com"

Impersonal Message
Be wary if a company with which you regularly do business fails to address you by name

Prof Santosh Chapaneri,
santoshchapaneri@gmail.com

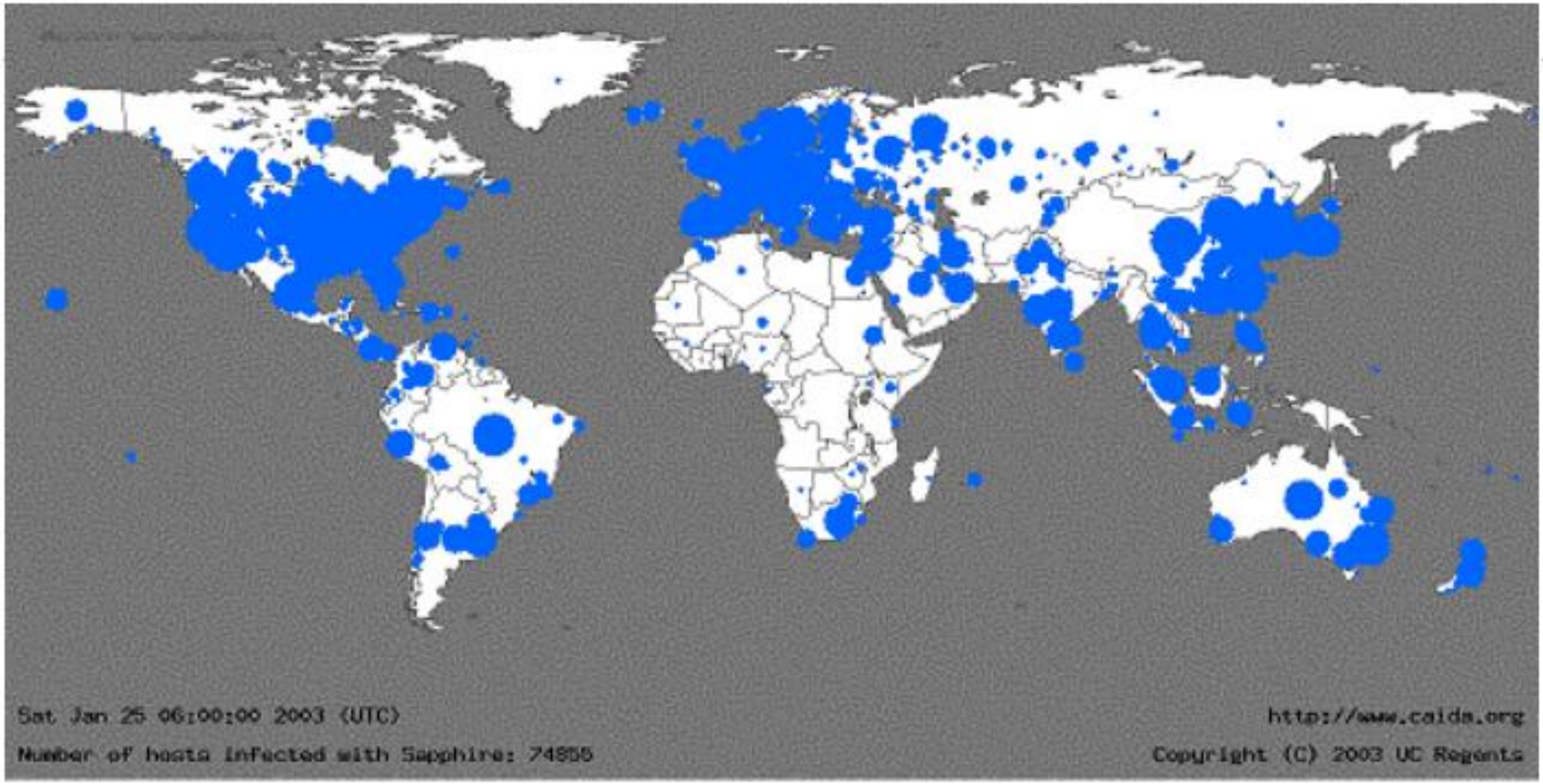
Security: Counter-measures

Question:
How do you stop a bullet that has already been fired?



Bullet goes verryy fast

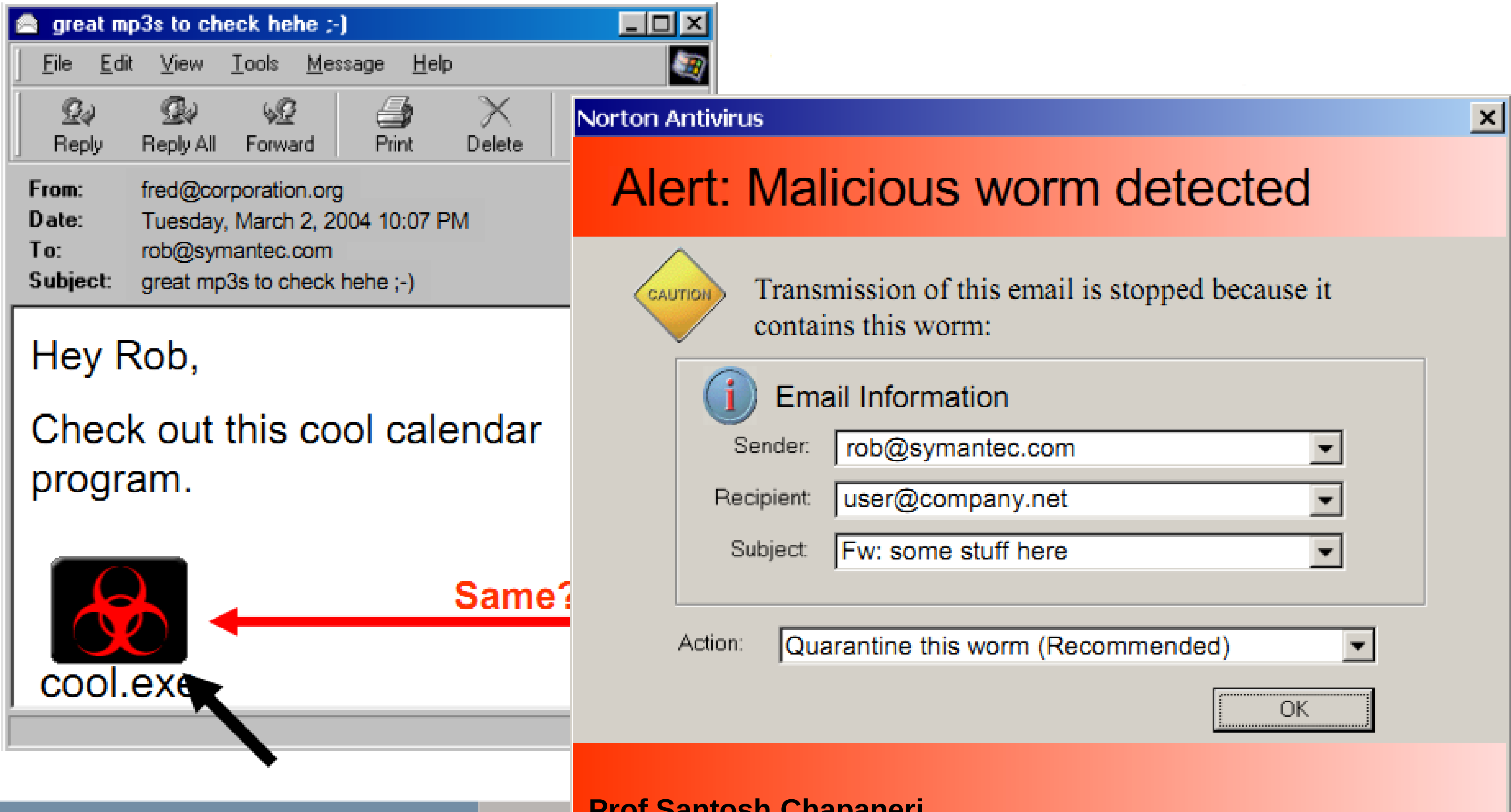
Typical Worm Attack Scenario



- Spread of SQL Slammer worm 8 minutes after its deployment
- 150,000 – 200,000 servers worldwide have been infected

Symantec Norton Anti-Virus

- Symantec pushes up to 1.4 billion virus signature updates every day! That is up to 60 TB of data send every day.

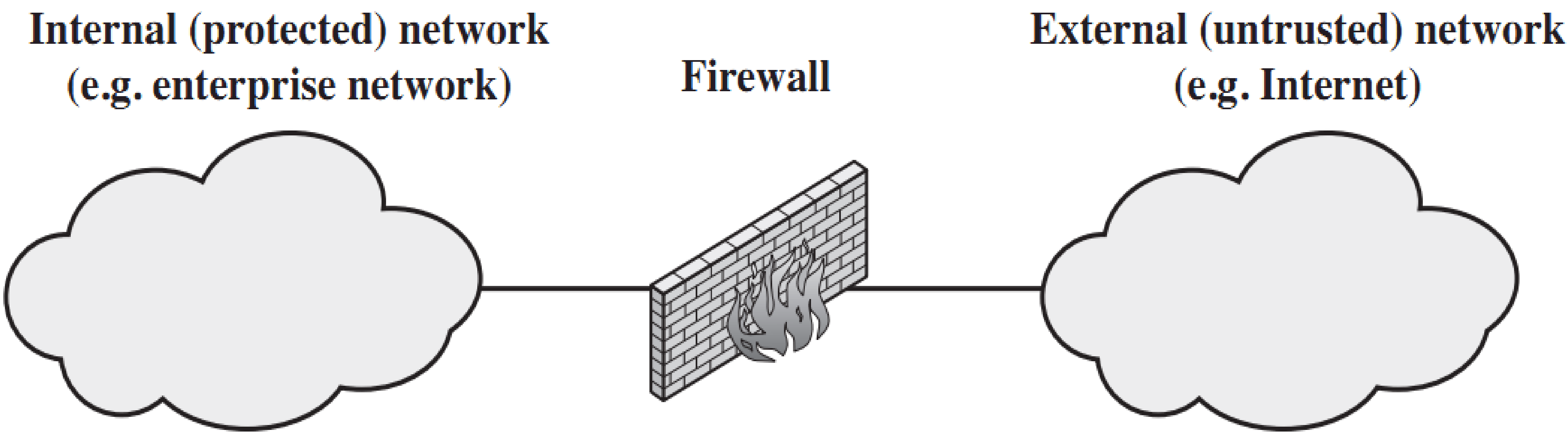


Prof Santosh Chapaneri, santoshchapaneri@gmail.com

Microsoft Windows Anti-Spyware

Firewalls

- A firewall forms a **barrier** through which the traffic going in each direction must pass. A firewall security policy dictates which traffic is authorized to pass in each direction.
- A firewall may be designed to operate as a filter at the level of IP packets, or may operate at a higher protocol layer.



Example: Personal Firewall Interface

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Network 3
Notification state:	Notify me when Windows Firewall blocks a new program

Thank You

References

- B. Furht, and D. Kivorski, *Multimedia Security Handbook*, 2004
- T. Yang, C. Wu, and L. Chua, “Cryptography based on chaotic systems”, IEEE Trans. on Circuits and Systems, vol. 44, 1997
- W. Diffie, and M. Hellman, “New directions in Cryptography”, IEEE Trans. Information Theory, 1976
- W. Stallings, *Network and Internetwork Security Principles and Practice*, Prentice Hall, 1995
- B. Schneier, *Applied Cryptography*, John Wiley, New York, 1996
- Y. Mao, G. Chen, S. Lian, “A novel fast image encryption scheme based on the 3D chaotic baker map”, *Intl. Journal Bifurcation & Chaos*, Vol. 14, 2004
- S. Bhargava, “A fast MPEG video encryption algorithm”, *Proc 6th ACM Intl Multimedia Conference*, UK, 1998
- W. Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, NJ, 2003
- J. Shah, and V. Saxena, “Video encryption: A survey”, *Intl Journal of Computer Science Issues*, Vol. 8, Issue 2, Mar 2011

Example: Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

RSA Example: Confidentiality

- Take $p = 7$, $q = 11$, so $n = 77$ and $\phi(n) = 60$
- Alice chooses $e = 17$, making $d = 53$
- Bob wants to send Alice secret message HELLO (07 04 11 11 14)
  - $07^{17} \bmod 77 = 28$
  - $04^{17} \bmod 77 = 16$
  - $11^{17} \bmod 77 = 44$
  - $11^{17} \bmod 77 = 44$
  - $14^{17} \bmod 77 = 42$
- Bob sends 28 16 44 44 42

RSA Example: Confidentiality (contd.)

- Alice receives 28 16 44 44 42
- Alice uses private key, $d = 53$, to decrypt message:
  - $28^{53} \bmod 77 = 07$
  - $16^{53} \bmod 77 = 04$
  - $44^{53} \bmod 77 = 11$
  - $44^{53} \bmod 77 = 11$
  - $42^{53} \bmod 77 = 14$
- Alice translates message to letters to read HELLO
  - No one else could read it, as only Alice knows her private key and that is needed for decryption

RSA Example: Authentication

- Take $p = 7$, $q = 11$, so $n = 77$ and $\phi(n) = 60$
- Alice chooses $e = 17$, making $d = 53$
- Alice wants to send Bob message HELLO (07 04 11 11 14) so Bob knows it is what Alice sent (no changes in transit, and authenticated)
  - $07^{53} \bmod 77 = 35$
  - $04^{53} \bmod 77 = 09$
  - $11^{53} \bmod 77 = 44$
  - $11^{53} \bmod 77 = 44$
  - $14^{53} \bmod 77 = 49$
- Alice sends 35 09 44 44 49

RSA Example: Authentication (contd.)

- Bob receives 35 09 44 44 49
- Bob uses Alice's public key, $e = 17$, $n = 77$, to decrypt message:
  - $35^{17} \bmod 77 = 07$
  - $09^{17} \bmod 77 = 04$
  - $44^{17} \bmod 77 = 11$
  - $44^{17} \bmod 77 = 11$
  - $49^{17} \bmod 77 = 14$
- Bob translates message to letters to read HELLO
  - Alice sent it as only she knows her private key, so no one else could have enciphered it
  - If (enciphered) message's blocks (letters) altered in transit, would not decrypt properly

RSA Example: Confidentiality + Authentication

- Alice wants to send Bob message HELLO both enciphered and authenticated (integrity-checked)
  - Alice's keys: public (17, 77); private: 53
  - Bob's keys: public: (37, 77); private: 13
- Alice enciphers HELLO (07 04 11 11 14):
  - $(07^{53} \bmod 77)^{37} \bmod 77 = 07$
  - $(04^{53} \bmod 77)^{37} \bmod 77 = 37$
  - $(11^{53} \bmod 77)^{37} \bmod 77 = 44$
  - $(11^{53} \bmod 77)^{37} \bmod 77 = 44$
  - $(14^{53} \bmod 77)^{37} \bmod 77 = 14$
- Alice sends 07 37 44 44 14