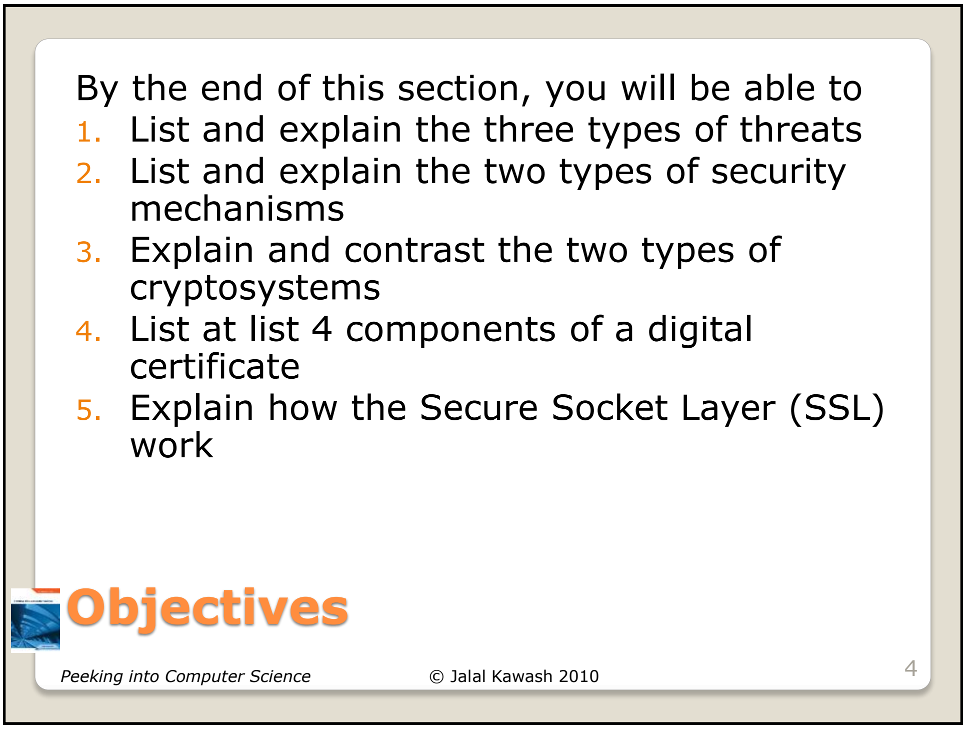
Networking & Security

Peeking into Computer Science

- Mandatory: Section 6.2

Reading Assignment

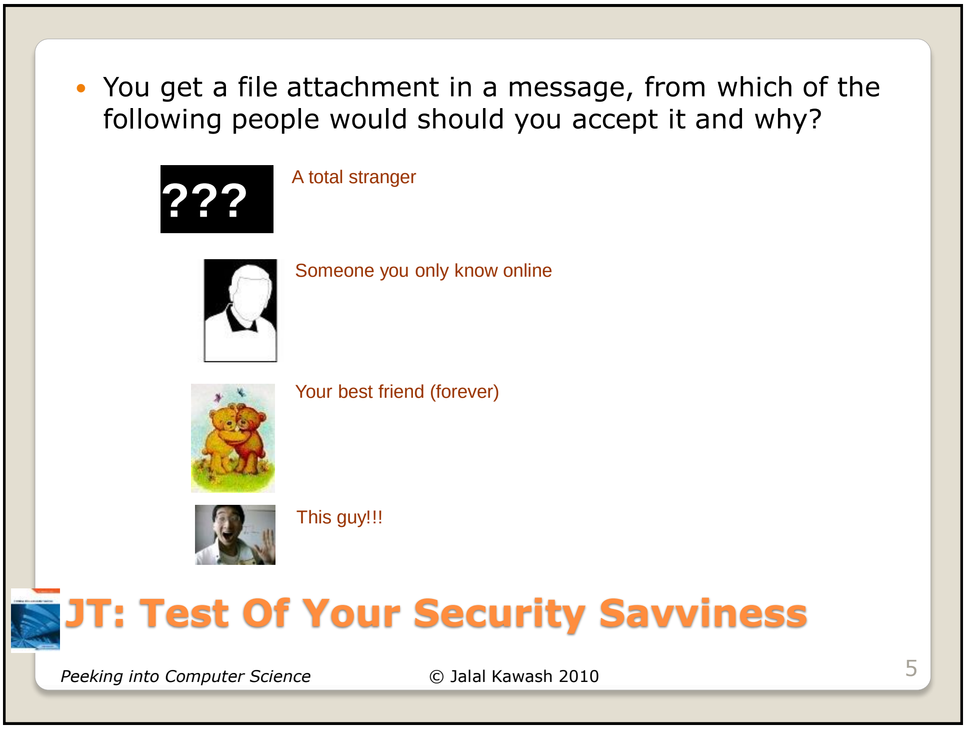
Secure Channels & Authentication



Objectives

By the end of this section, you will be able to

1. List and explain the three types of threats
2. List and explain the two types of security mechanisms
3. Explain and contrast the two types of cryptosystems
4. List at list 4 components of a digital certificate
5. Explain how the Secure Socket Layer (SSL) work



JT: Test Of Your Security Savviness

- You get a file attachment in a message, from which of the following people would should you accept it and why?

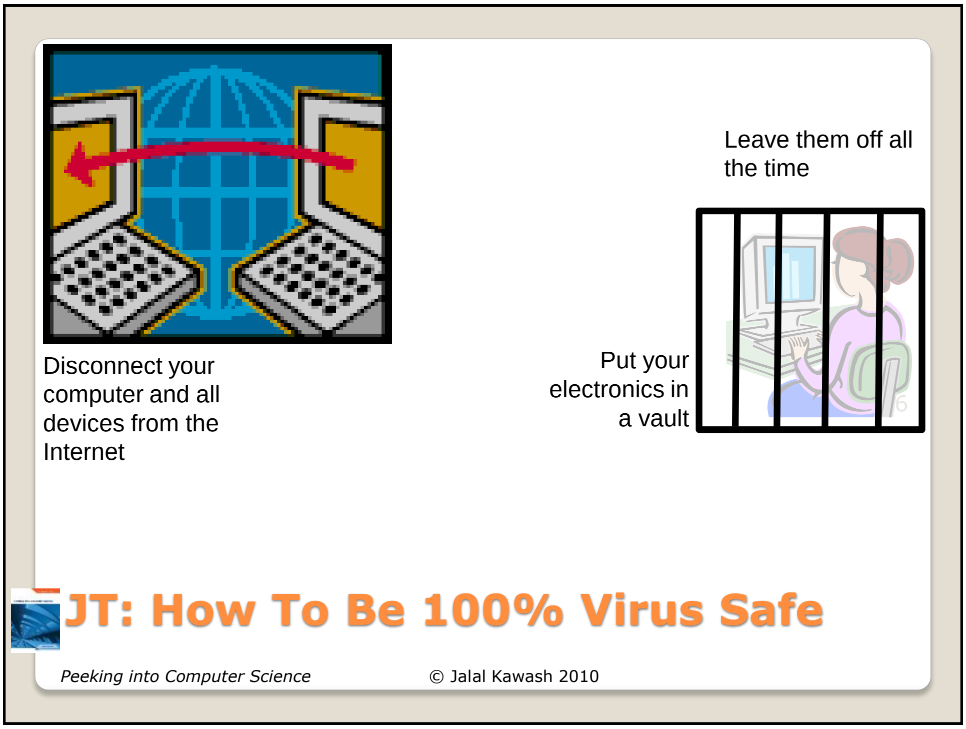
???

A total stranger

Someone you only know online

Your best friend (forever)

This guy!!!



JT: How To Be 100% Virus Safe

Disconnect your computer and all devices from the Internet

Leave them off all the time

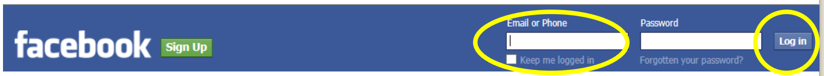
Put your electronics in a vault

JT: Lesson Learned

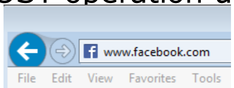
- You are never guaranteed to have 100% protection.
- What taking precautions (e.g., getting anti-virus software) provide is a *reduced* chance of an infection or other security-related problem.

JT: When A Threat Can Occur

- Recall that there are two web interactions previously covered:
  - GET: click on a link
  - POST: sending information on the web

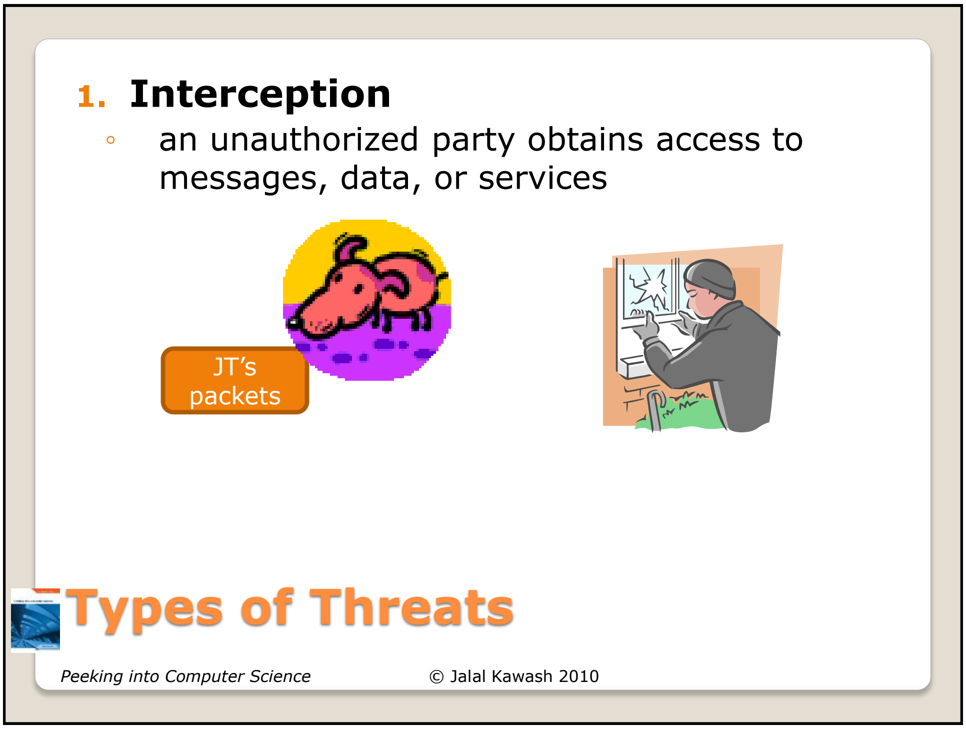


- During a POST operation using regular web protocols:



…whatever information you post (information you have filled in) may be intercepted.

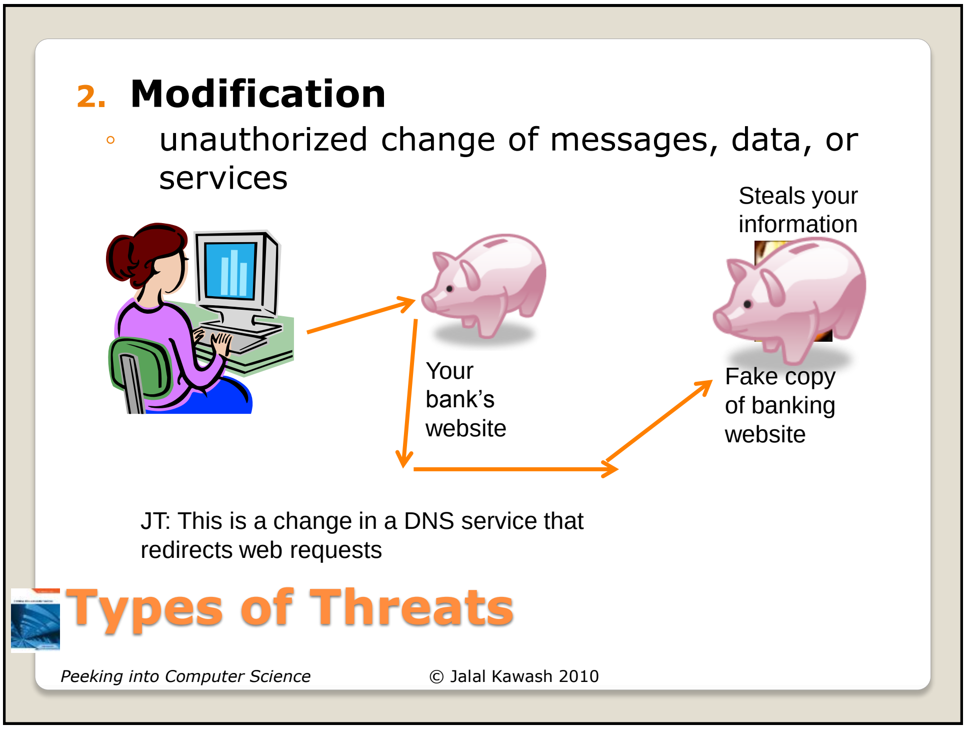
"Packet sniffing" (viewing contents): http://www.wikihow.com/Sniff-Packets



Types of Threats

1. **Interception**
   - an unauthorized party obtains access to messages, data, or services

JT's packets



Types of Threats

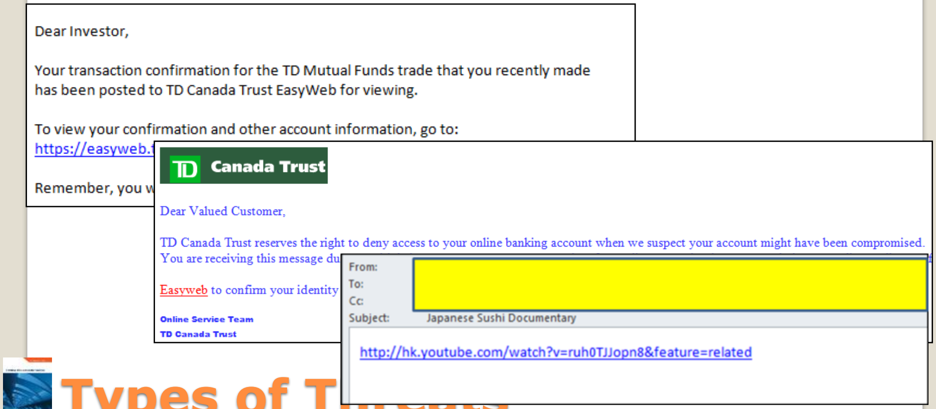
2. **Modification**
   - unauthorized change of messages, data, or services

Steals your information
Your bank's website
Fake copy of banking website

JT: This is a change in a DNS service that redirects web requests

3. Fabrication

- unauthorized creation of messages, data, or services
  - JT: Real or fake?



Dear Investor,

Your transaction confirmation for the TD Mutual Funds trade that you recently made has been posted to TD Canada Trust EasyWeb for viewing.

To view your confirmation and other account information, go to:
https://easyweb.t

Remember, you w

TD Canada Trust

Dear Valued Customer,

TD Canada Trust reserves the right to deny access to your online banking account when we suspect your account might have been compromised. You are receiving this message du

Easyweb to confirm your identity

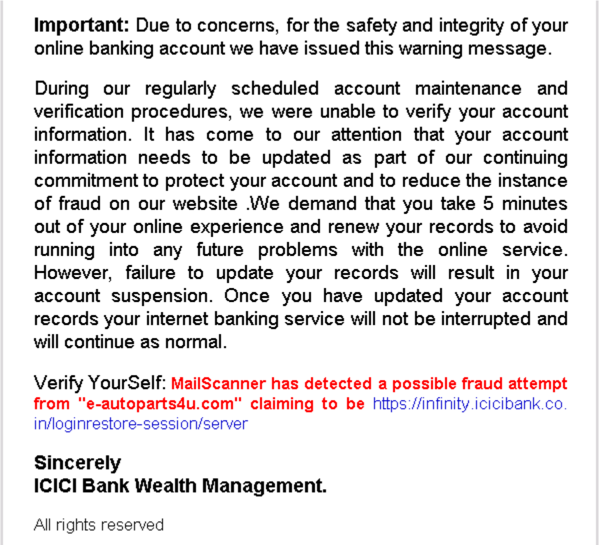
Online Service Team
TD Canada Trust

From: [redacted]
To:
Cc:
Subject: Japanese Sushi Documentary

http://hk.youtube.com/watch?v=ruh0TJJopn8&feature=related

Types of Threats

Peeking into Computer Science © Jalal Kawash 2010



Important: Due to concerns, for the safety and integrity of your online banking account we have issued this warning message.

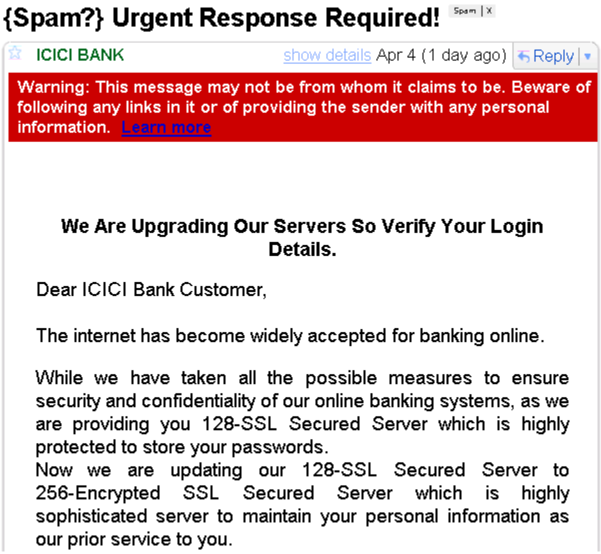
During our regularly scheduled account maintenance and verification procedures, we were unable to verify your account information. It has come to our attention that your account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website .We demand that you take 5 minutes out of your online experience and renew your records to avoid running into any future problems with the online service. However, failure to update your records will result in your account suspension. Once you have updated your account records your internet banking service will not be interrupted and will continue as normal.

Verify YourSelf: **MailScanner has detected a possible fraud attempt from "e-autoparts4u.com" claiming to be** https://infinity.icicibank.co.in/loginrestore-session/server

Sincerely
ICICI Bank Wealth Management.

All rights reserved

Peeking into Computer Science © Jalal Kawash 2009 12



{Spam?} Urgent Response Required!

ICICI BANK show details Apr 4 (1 day ago) Reply

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

We Are Upgrading Our Servers So Verify Your Login Details.

Dear ICICI Bank Customer,

The internet has become widely accepted for banking online.

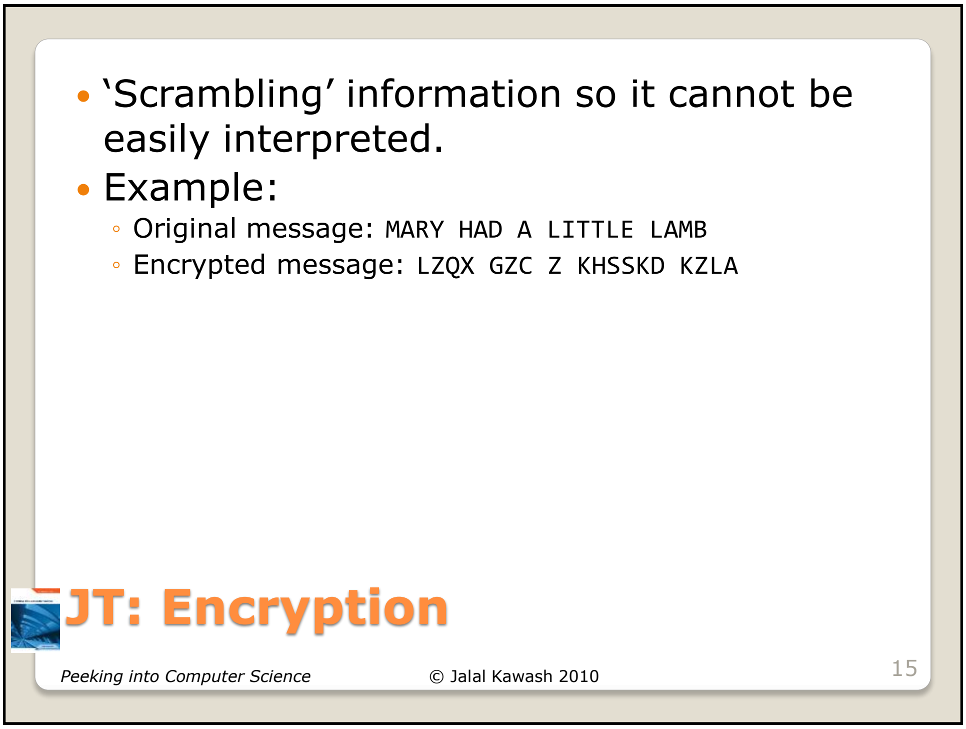
While we have taken all the possible measures to ensure security and confidentiality of our online banking systems, as we are providing you 128-SSL Secured Server which is highly protected to store your passwords.
Now we are updating our 128-SSL Secured Server to 256-Encrypted SSL Secured Server which is highly sophisticated server to maintain your personal information as our prior service to you.

Peeking into Computer Science © Jalal Kawash 2009 13

1. **Encryption**
   - encode data and messages so that only intended parties can decode them
2. **Authentication**
   - verify that the claimed identity by some party is authentic

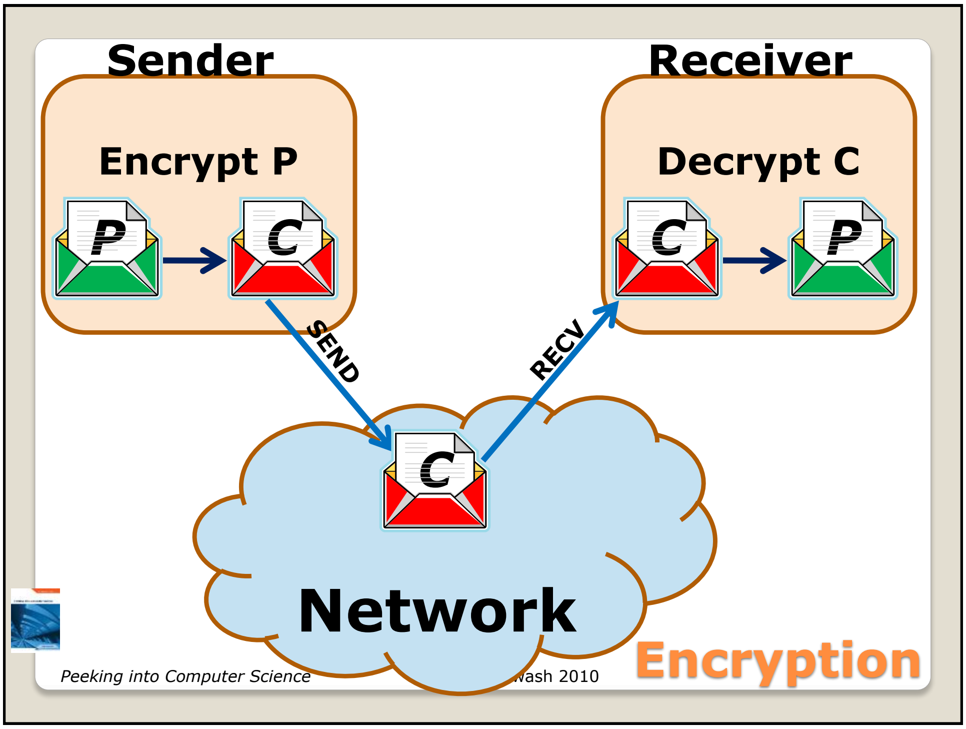
Security Measures against Threats

Peeking into Computer Science © Jalal Kawash 2010



JT: Encryption

- ‘Scrambling’ information so it cannot be easily interpreted.
- Example:
  - Original message: `MARY HAD A LITTLE LAMB`
  - Encrypted message: `LZQX GZC Z KHSSKD KZLA`



Encryption

Sender

Encrypt P

P → C

SEND

Receiver

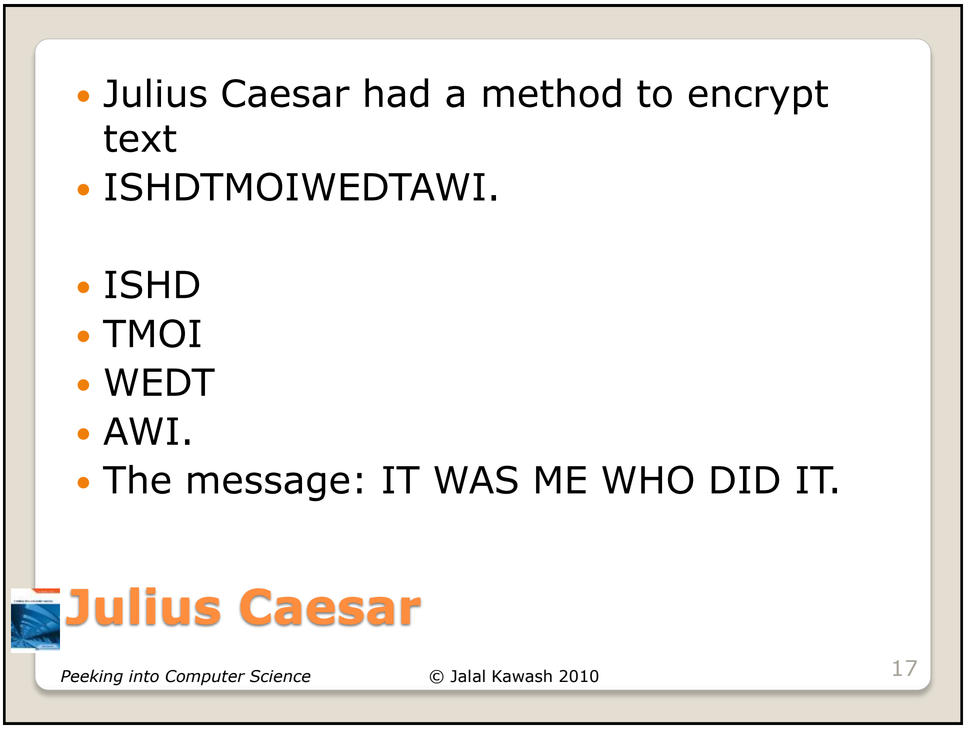
Decrypt C

C → P

RECV

C

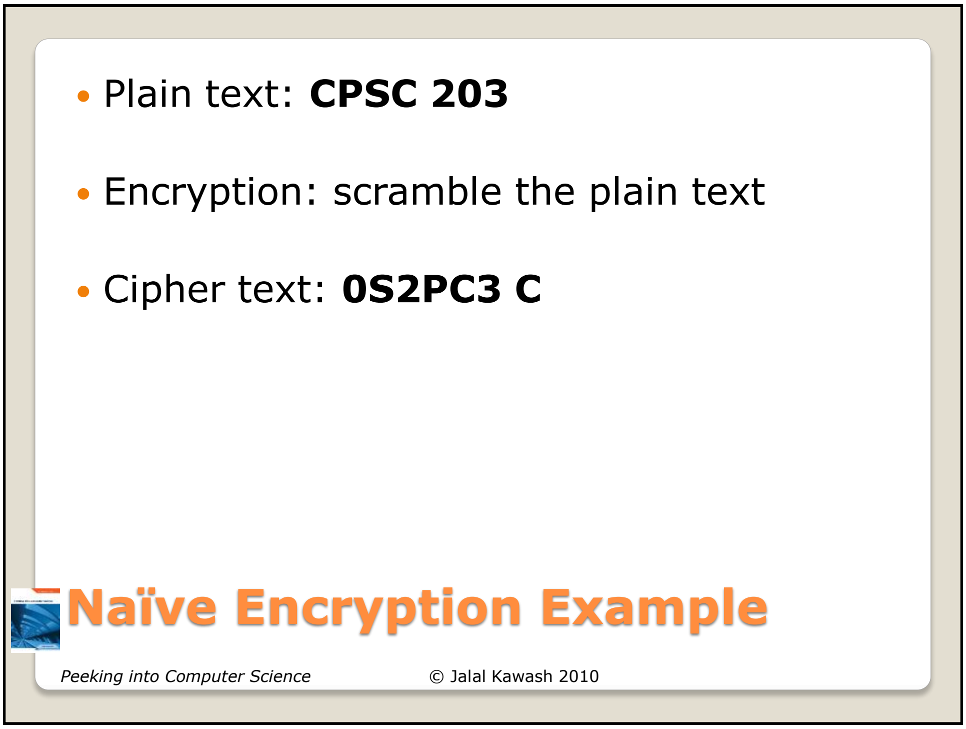
Network



Julius Caesar

- Julius Caesar had a method to encrypt text
- ISHDTMOIWEDTAWI.

- ISHD
- TMOI
- WEDT
- AWI.
- The message: IT WAS ME WHO DID IT.

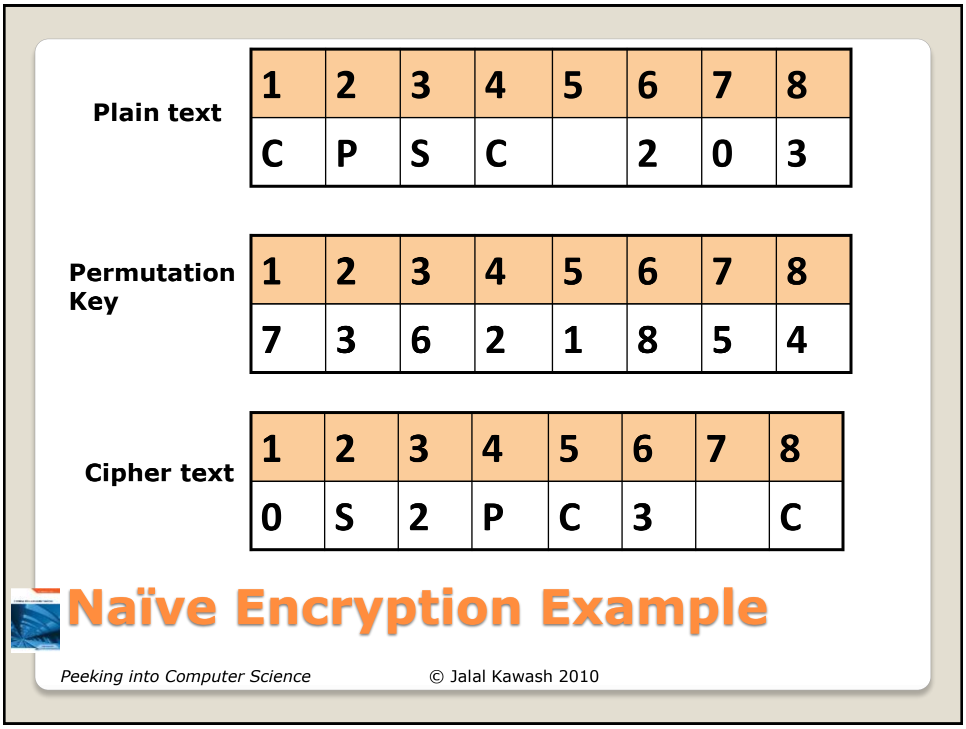


Naïve Encryption Example

- Plain text: **CPSC 203**

- Encryption: scramble the plain text

- Cipher text: **0S2PC3 C**



Naïve Encryption Example

Plain text

1	2	3	4	5	6	7	8
C	P	S	C		2	0	3

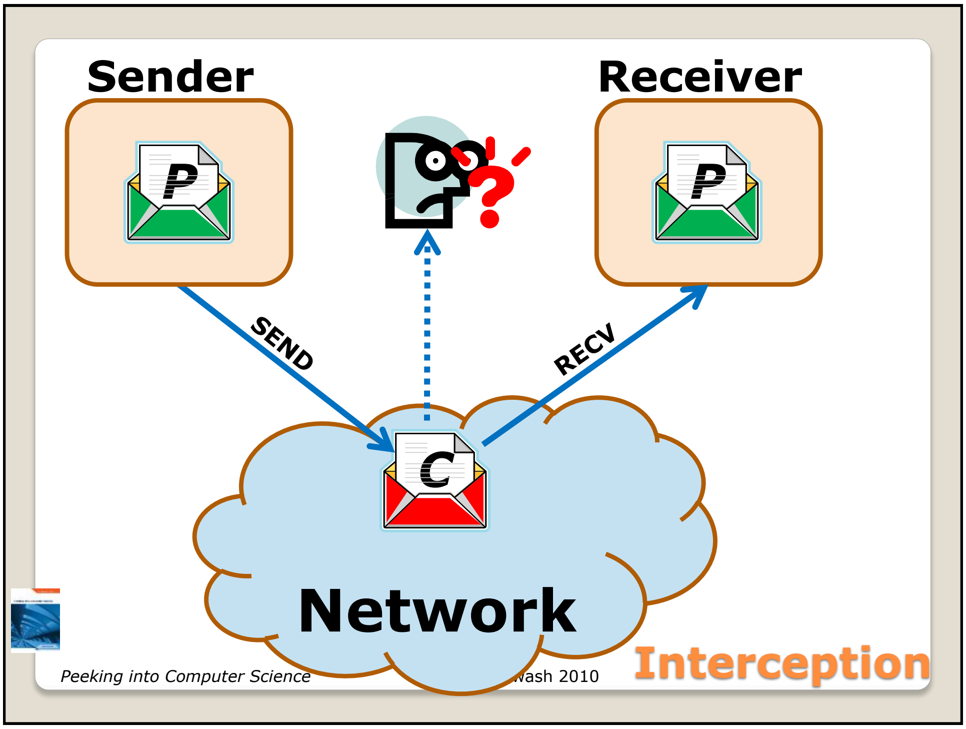
Permutation Key

1	2	3	4	5	6	7	8
7	3	6	2	1	8	5	4

Cipher text

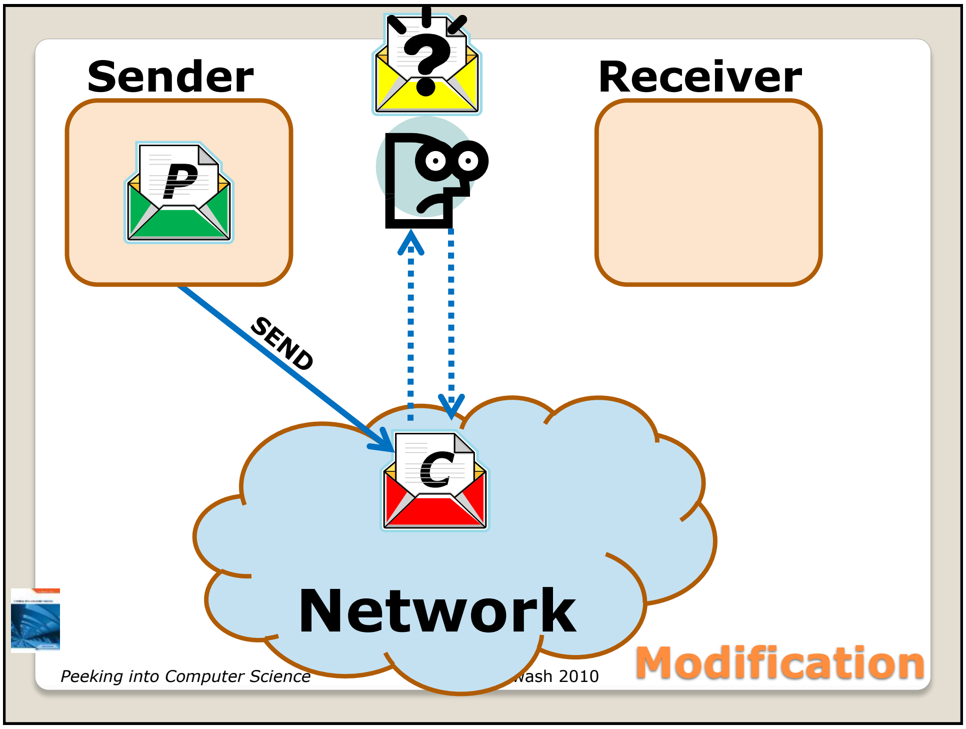
1	2	3	4	5	6	7	8
0	S	2	P	C	3		C

Peeking into Computer Science © Jalal Kawash 2010



Interception

Peeking into Computer Science wash 2010



Sender

Receiver

P

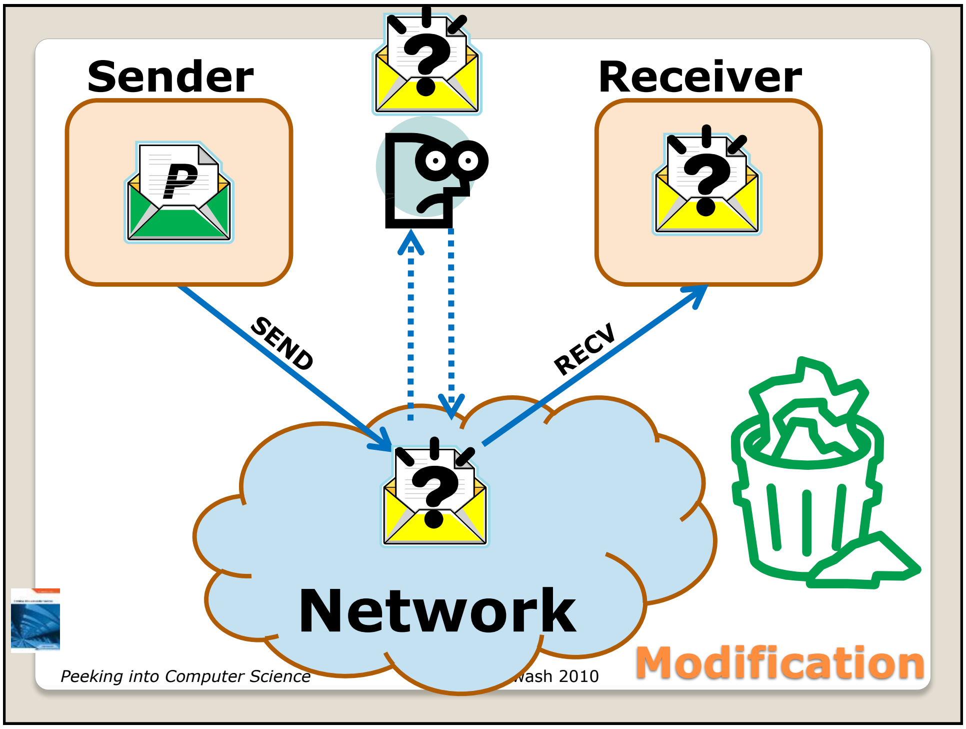
SEND

C

Network

Modification

Peeking into Computer Science ... Wash 2010



Sender

Receiver

P

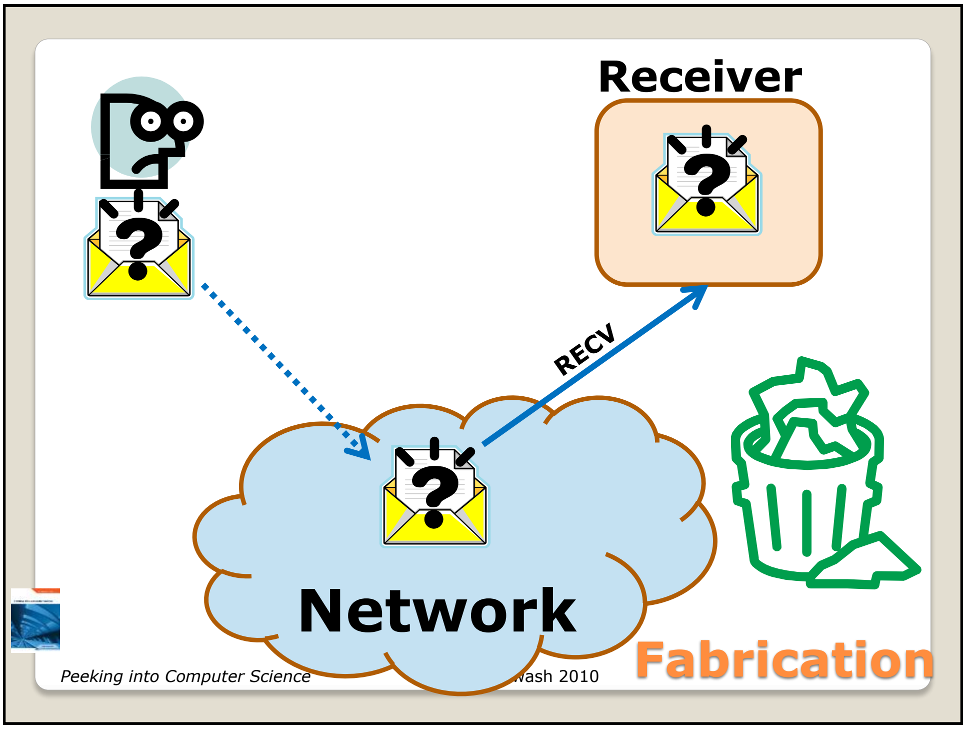
SEND

RECV

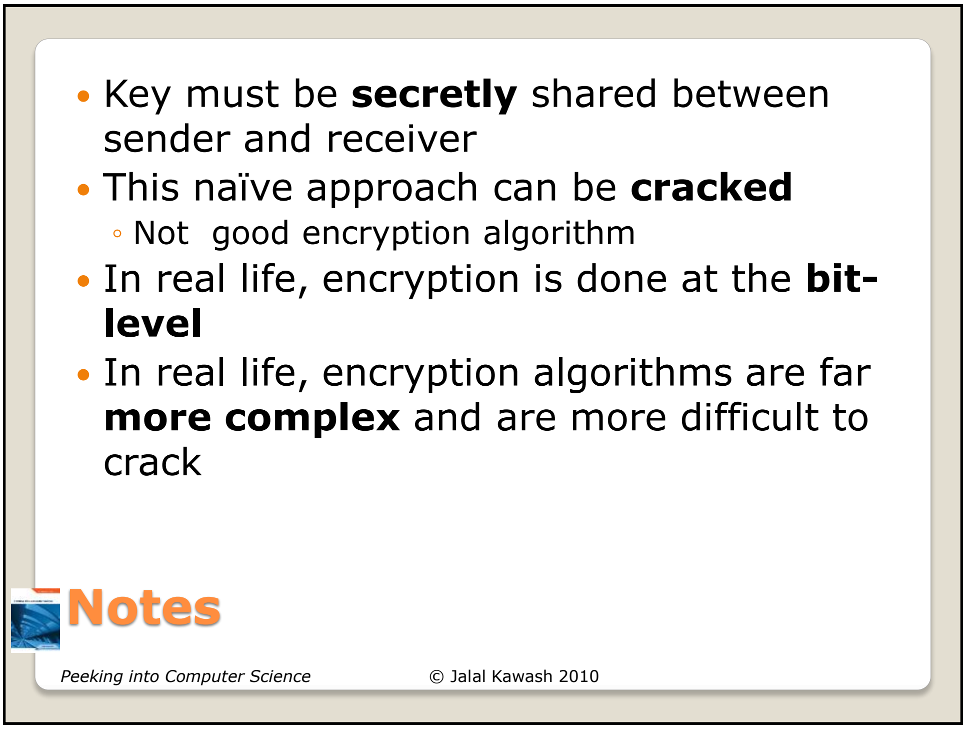
Network

Modification

Peeking into Computer Science ... Wash 2010

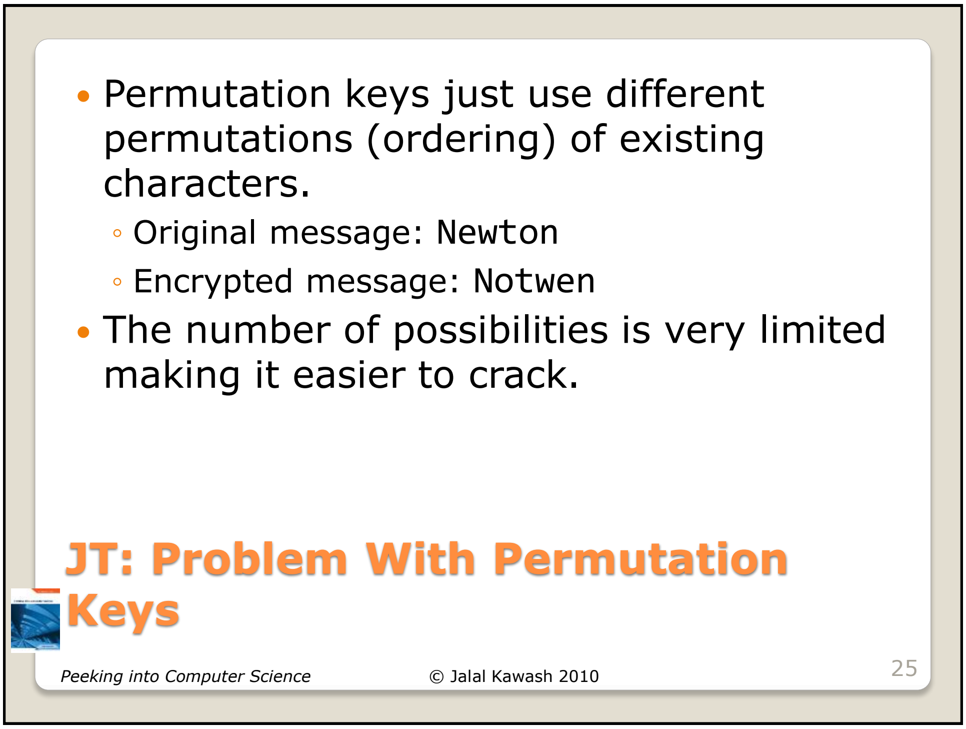


Peeking into Computer Science wash 2010


- Key must be **secretly** shared between sender and receiver
- This naïve approach can be **cracked**
  - Not good encryption algorithm
- In real life, encryption is done at the **bit-level**
- In real life, encryption algorithms are far **more complex** and are more difficult to crack

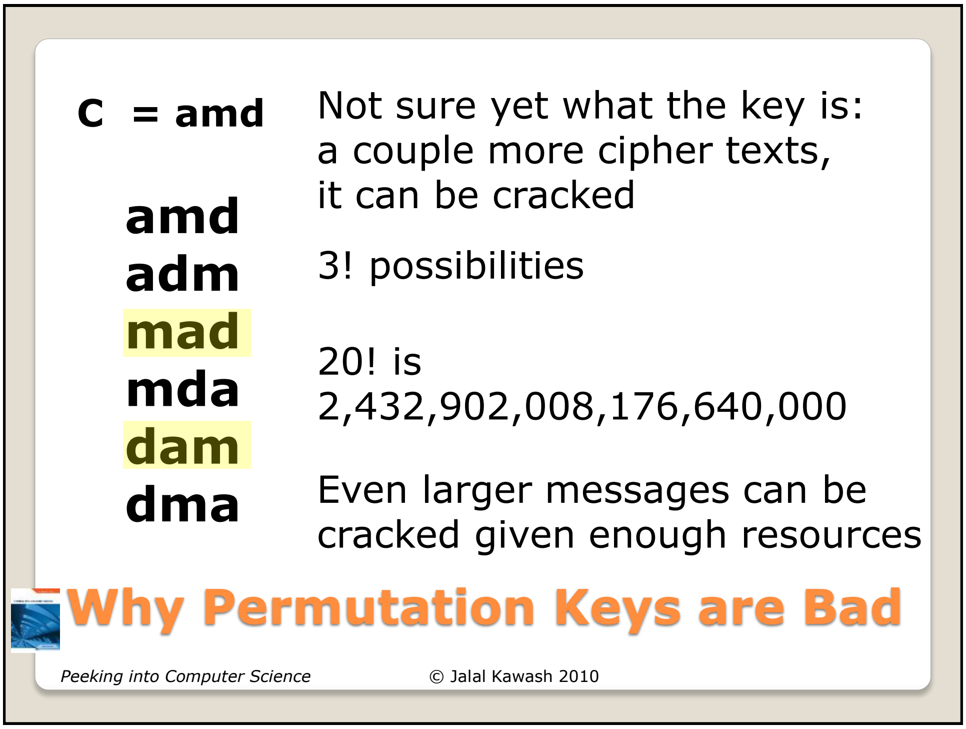
Notes

Peeking into Computer Science © Jalal Kawash 2010



JT: Problem With Permutation Keys

- Permutation keys just use different permutations (ordering) of existing characters.
  - Original message: Newton
  - Encrypted message: Notwen
- The number of possibilities is very limited making it easier to crack.



Why Permutation Keys are Bad

C = amd

amd
adm
mad
mda
dam
dma

Not sure yet what the key is:
a couple more cipher texts,
it can be cracked

3! possibilities

20! is
2,432,902,008,176,640,000

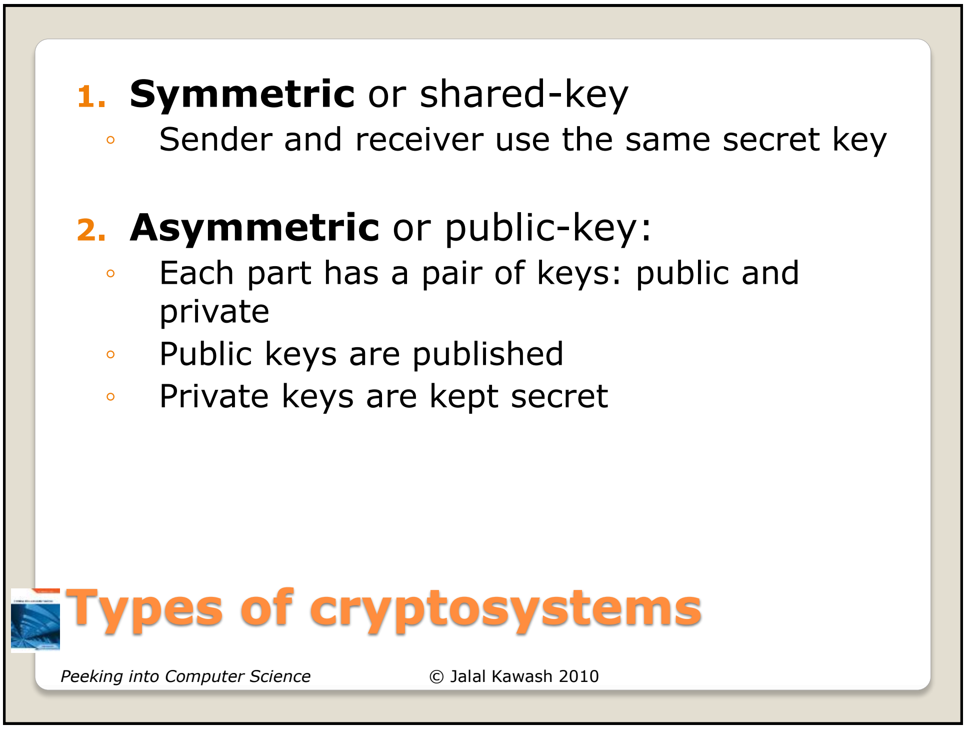
Even larger messages can be cracked given enough resources

JT: The Number Of Guesses Can Be Reduced

- Encryption is used to secure information e.g., financial, national defense, intelligence.
- Sometimes to speed up the decryption process only valid combinations will be attempted.
- Previous example: `AMD`
- In English the only valid combinations that need be examined: `MAD`, `DAM`
  - At first 3! attempts needed, this gets reduced down to 2 attempts needed.

JT: Longer/Complex Passwords Are Better For A Reason

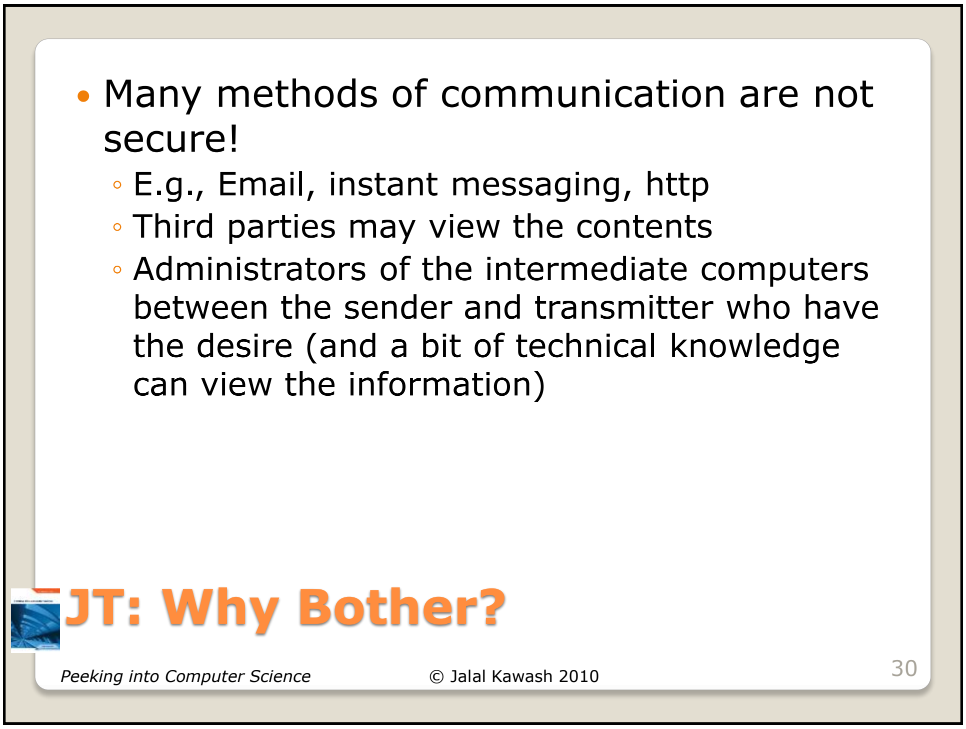
- More combinations means it’s harder to guess
  - Either it takes longer to crack or if it’s long and complex enough (with a good encryption algorithm) it will be practically impossible to try all combinations (sometimes tens of thousands of years).
- Guidelines for picking good passwords:
  - http://www.ucalgary.ca/it/help/articles/security/awareness/passwords



Types of cryptosystems

1. **Symmetric** or shared-key
   - Sender and receiver use the same secret key

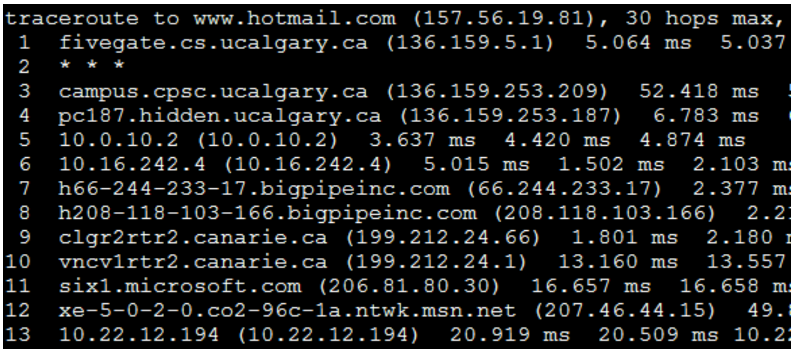
2. **Asymmetric** or public-key:
   - Each part has a pair of keys: public and private
   - Public keys are published
   - Private keys are kept secret



JT: Why Bother?

- Many methods of communication are not secure!
  - E.g., Email, instant messaging, http
  - Third parties may view the contents
  - Administrators of the intermediate computers between the sender and transmitter who have the desire (and a bit of technical knowledge can view the information)

- Example communication (my office computer to Microsoft’s Hotmail server)

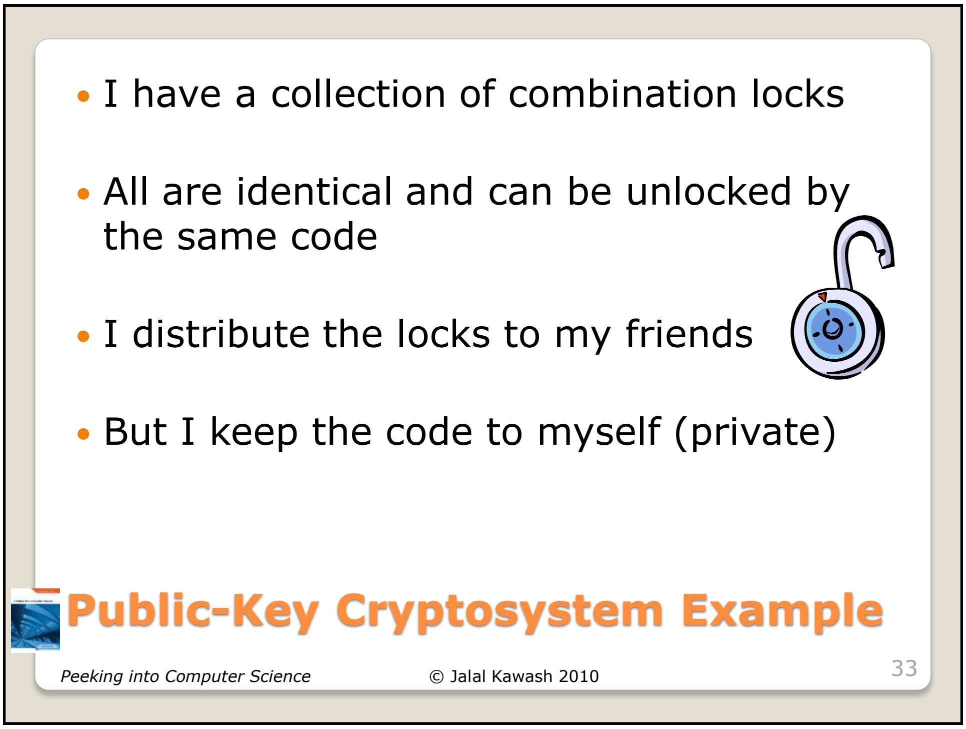


```
traceroute to www.hotmail.com (157.56.19.81), 30 hops max,
 1  fivegate.cs.ucalgary.ca (136.159.5.1)  5.064 ms  5.037
 2  * * *
 3  campus.cpsc.ucalgary.ca (136.159.253.209)  52.418 ms
 4  pc187.hidden.ucalgary.ca (136.159.253.187)  6.783 ms
 5  10.0.10.2 (10.0.10.2)  3.637 ms  4.420 ms  4.874 ms
 6  10.16.242.4 (10.16.242.4)  5.015 ms  1.502 ms  2.103 m
 7  h66-244-233-17.bigpipeinc.com (66.244.233.17)  2.377 m
 8  h208-118-103-166.bigpipeinc.com (208.118.103.166)  2.2
 9  clgr2rtr2.canarie.ca (199.212.24.66)  1.801 ms  2.180
10  vncv1rtr2.canarie.ca (199.212.24.1)  13.160 ms  13.557
11  six1.microsoft.com (206.81.80.30)  16.657 ms  16.658 m
12  xe-5-0-2-0.co2-96c-1a.ntwk.msn.net (207.46.44.15)  49.
13  10.22.12.194 (10.22.12.194)  20.919 ms  20.509 ms 10.2
```

JT: Why Bother?

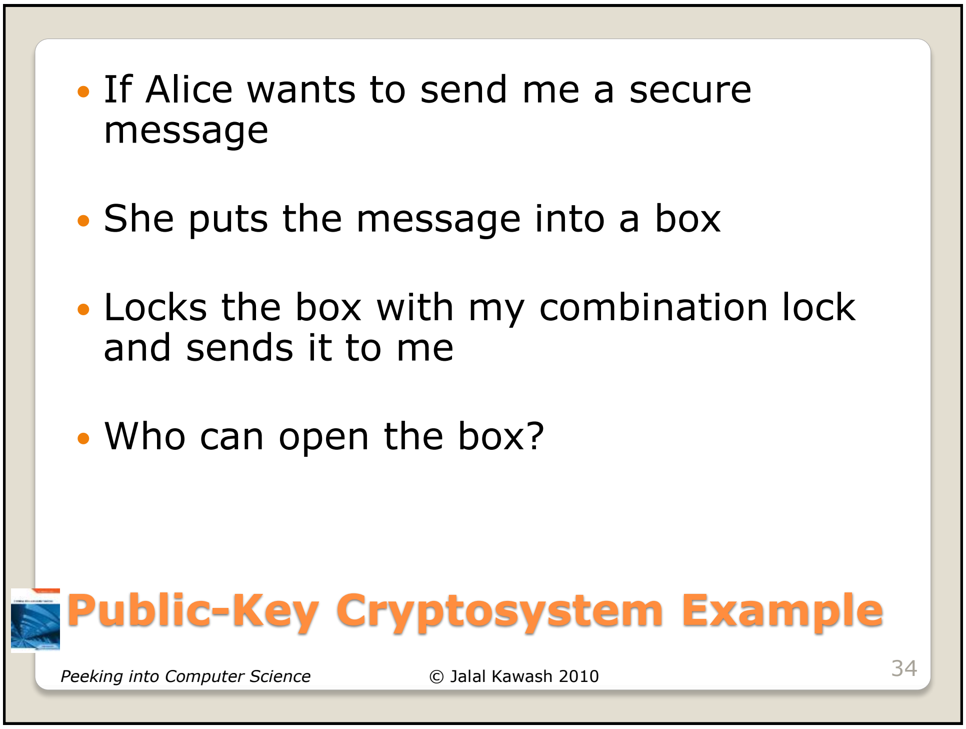
- There are two levels of security
- In the example that follows (securing the contents of a message):
  - The public key:
    - Anyone who wants to send the receiver a message can access it
    - Used to encrypt the data
    - It is sent along with the data
  - The private key
    - Only the receiver has a copy (should be kept inaccessible)
    - Decrypts the message for the receiver

JT: Public-Private Key Encryption



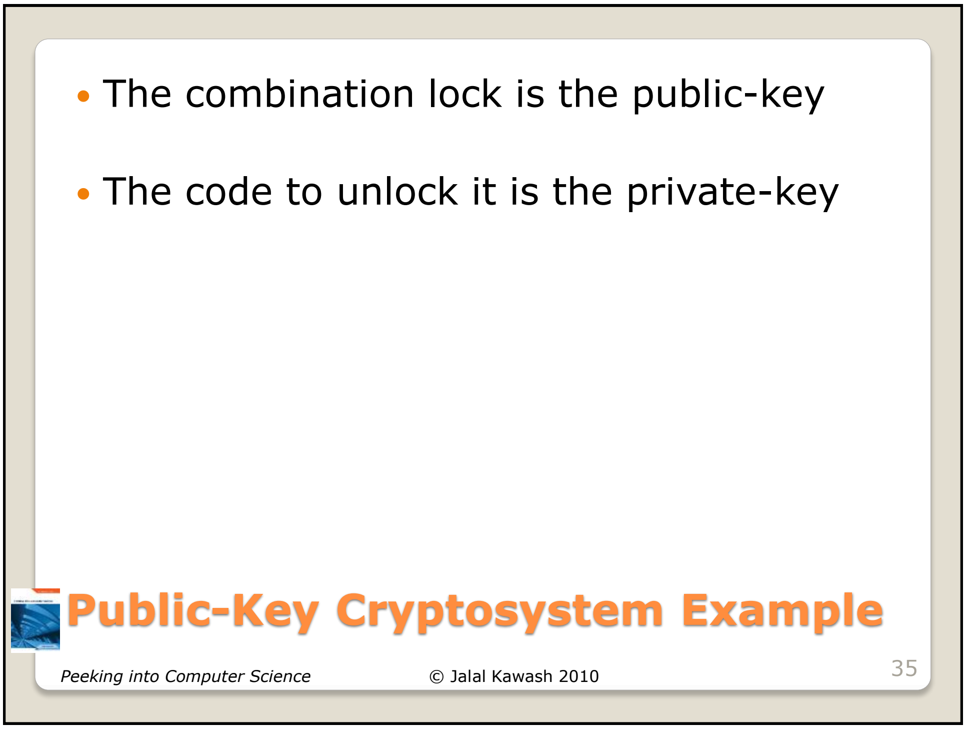
Public-Key Cryptosystem Example

- I have a collection of combination locks
- All are identical and can be unlocked by the same code
- I distribute the locks to my friends
- But I keep the code to myself (private)



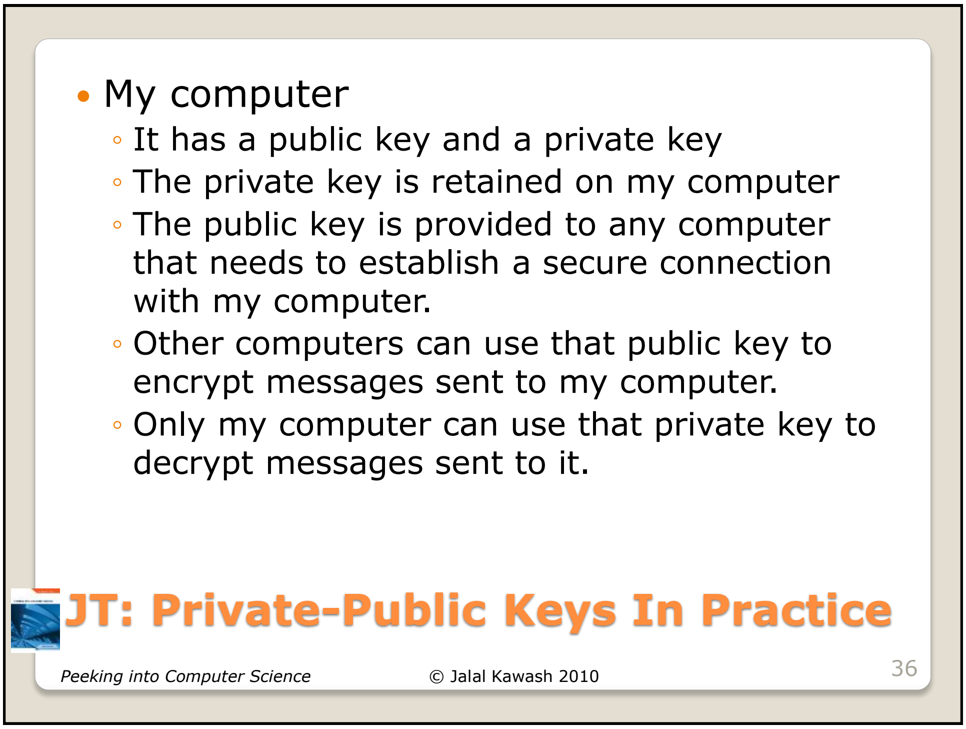
Public-Key Cryptosystem Example

- If Alice wants to send me a secure message
- She puts the message into a box
- Locks the box with my combination lock and sends it to me
- Who can open the box?



Public-Key Cryptosystem Example

- The combination lock is the public-key
- The code to unlock it is the private-key



JT: Private-Public Keys In Practice

- My computer
  - It has a public key and a private key
  - The private key is retained on my computer
  - The public key is provided to any computer that needs to establish a secure connection with my computer.
  - Other computers can use that public key to encrypt messages sent to my computer.
  - Only my computer can use that private key to decrypt messages sent to it.

- X's public key is denoted K_X^+
- X's private key is denoted K_X^-

- K_X^+ and K_X^- are reciprocal
  - JT: Normally done this way
    - Cipher text: C = Encrypt(P, K_X^+) ← Sender
    - Plaintext: P = Decrypt(C, K_X^-) ← Receiver
  - JT: Normally NOT done this way (it's just included to be complete)
    - Cipher text: C = Encrypt(P, K_X^-) ← Sender
    - Plaintext: P= Decrypt(C, K_X^+) ← Receiver

Public and private keys

- Sender **S,** receiver **R**

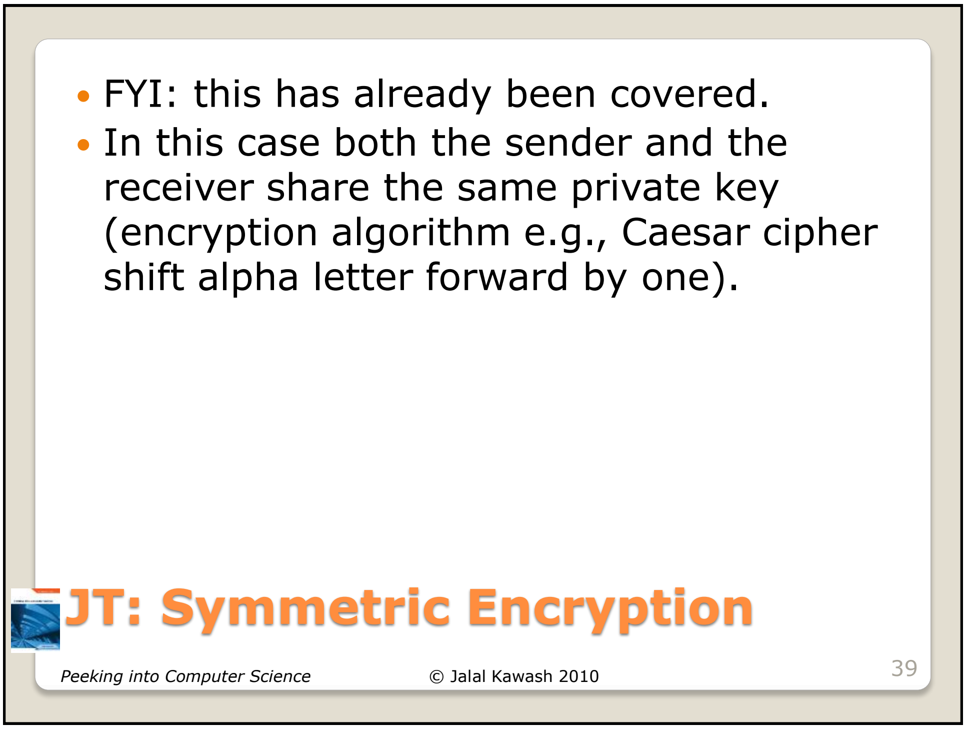
- **S** sends **R** the secure message

  C = Encrypt(P, K_R^+)

- Only **R** knows K_R^- and can decrypt C

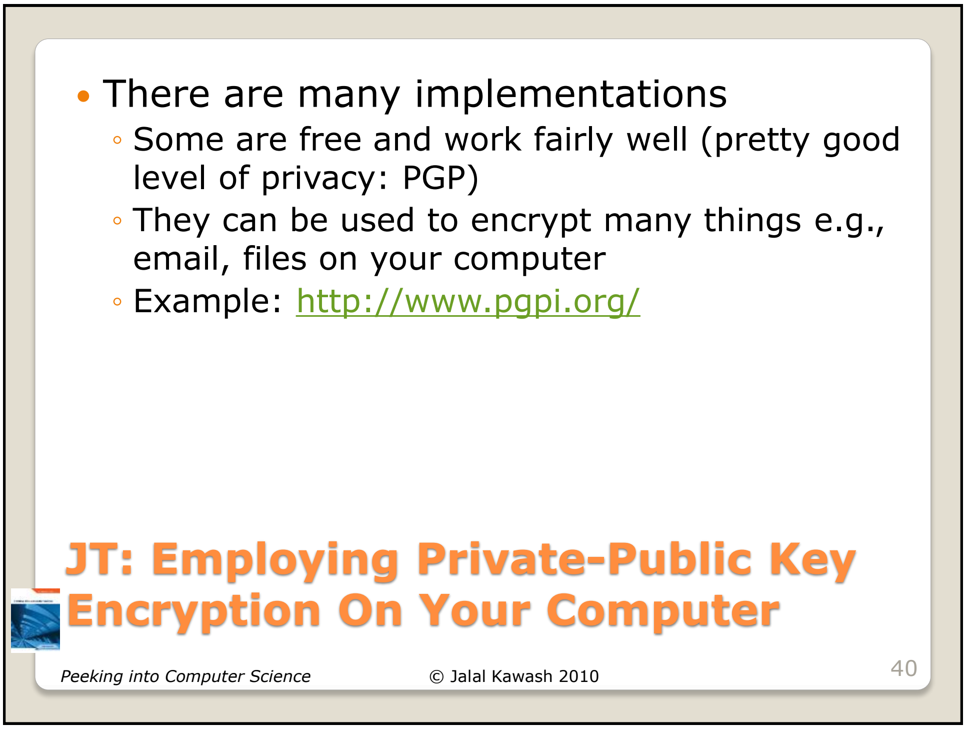
  P = Decrypt(C, K_R^-)

Asymmetric encryption



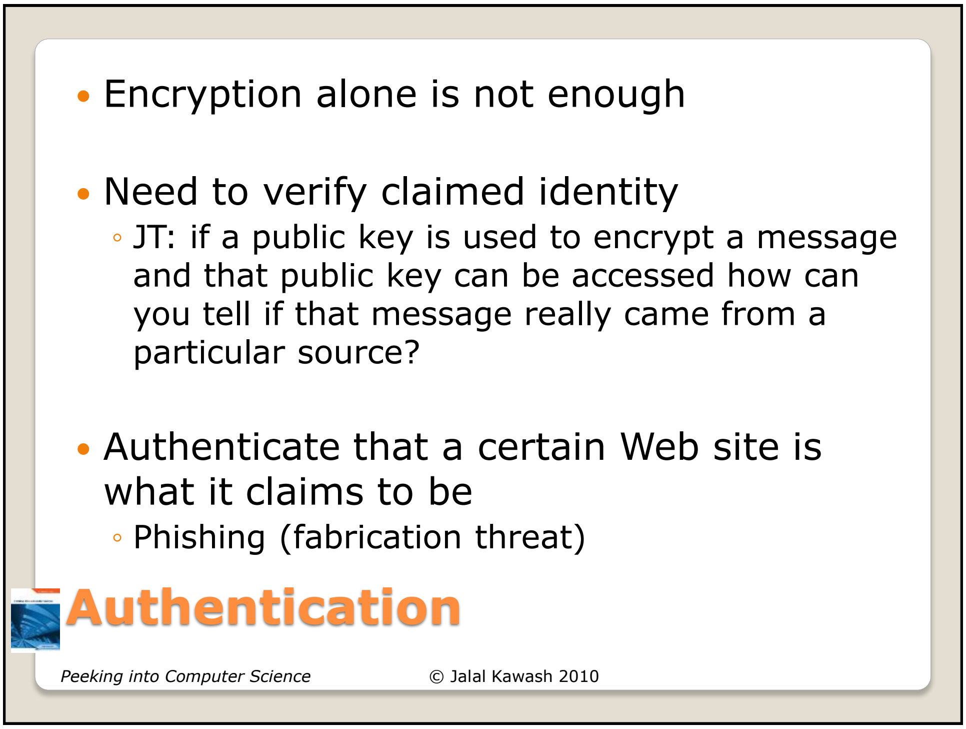
JT: Symmetric Encryption

- FYI: this has already been covered.
- In this case both the sender and the receiver share the same private key (encryption algorithm e.g., Caesar cipher shift alpha letter forward by one).



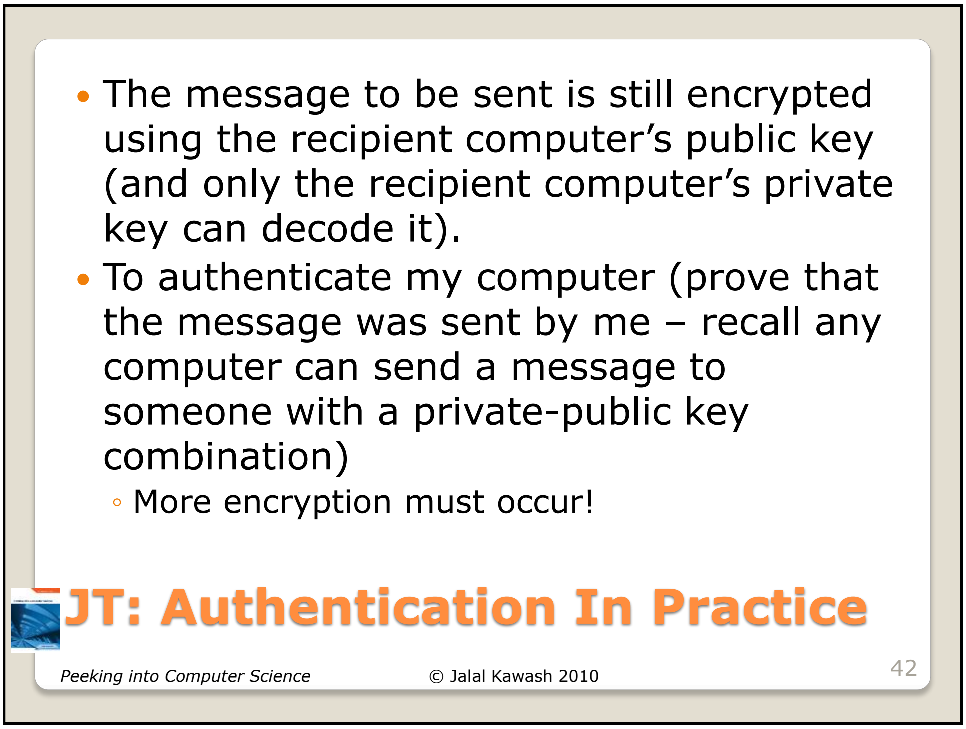
JT: Employing Private-Public Key Encryption On Your Computer

- There are many implementations
  - Some are free and work fairly well (pretty good level of privacy: PGP)
  - They can be used to encrypt many things e.g., email, files on your computer
  - Example: http://www.pgpi.org/



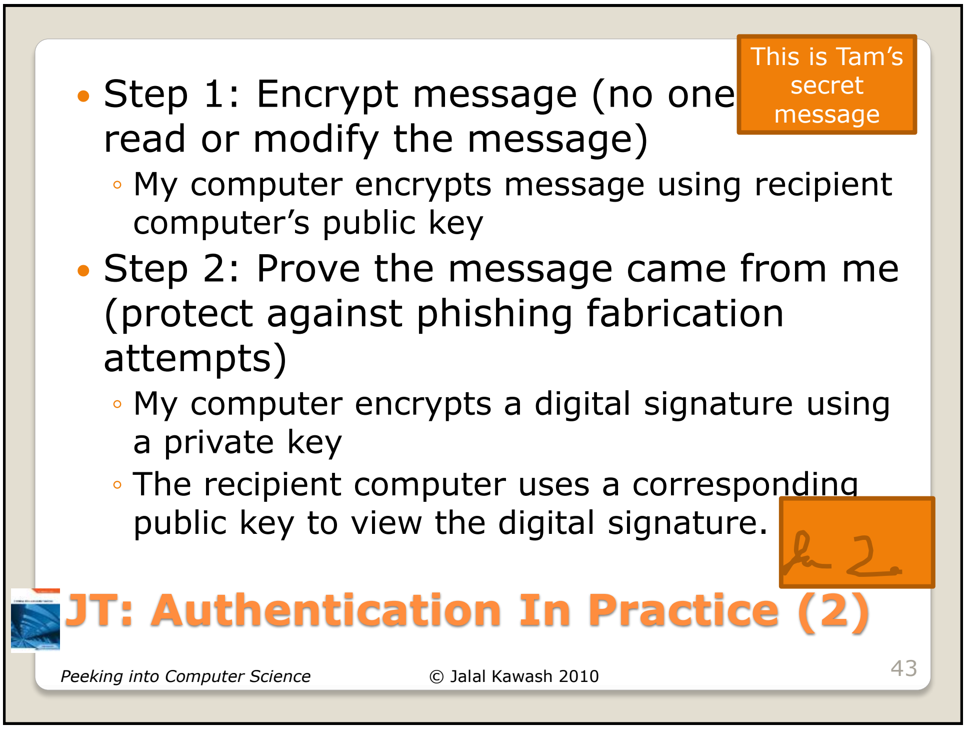
Authentication

- Encryption alone is not enough
- Need to verify claimed identity
  - JT: if a public key is used to encrypt a message and that public key can be accessed how can you tell if that message really came from a particular source?
- Authenticate that a certain Web site is what it claims to be
  - Phishing (fabrication threat)



JT: Authentication In Practice

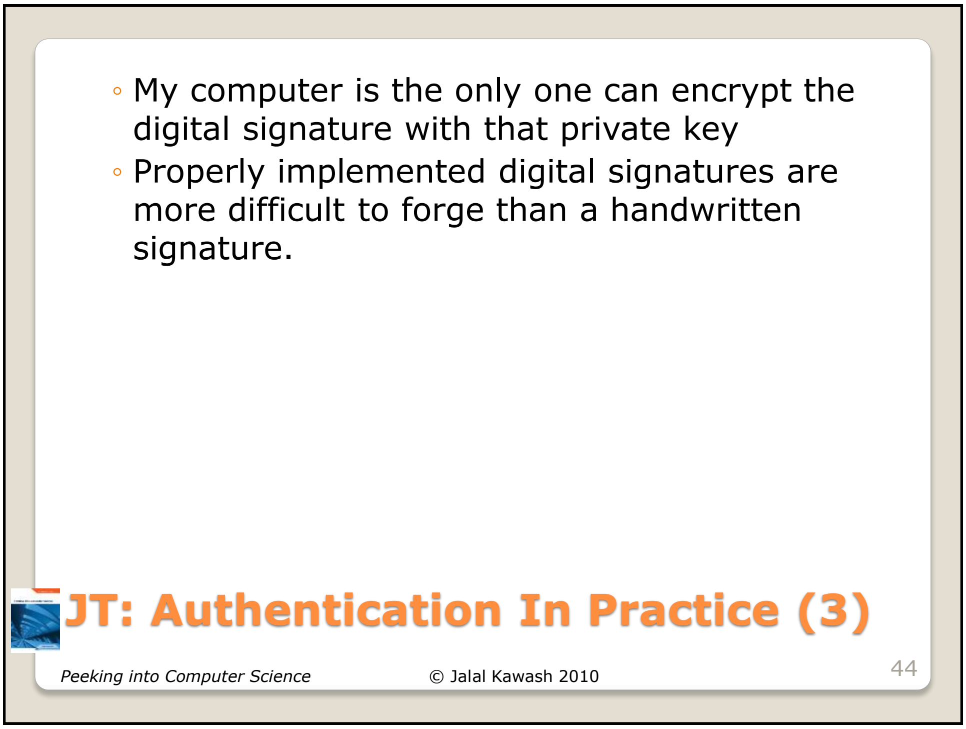
- The message to be sent is still encrypted using the recipient computer’s public key (and only the recipient computer’s private key can decode it).
- To authenticate my computer (prove that the message was sent by me – recall any computer can send a message to someone with a private-public key combination)
  - More encryption must occur!



JT: Authentication In Practice (2)

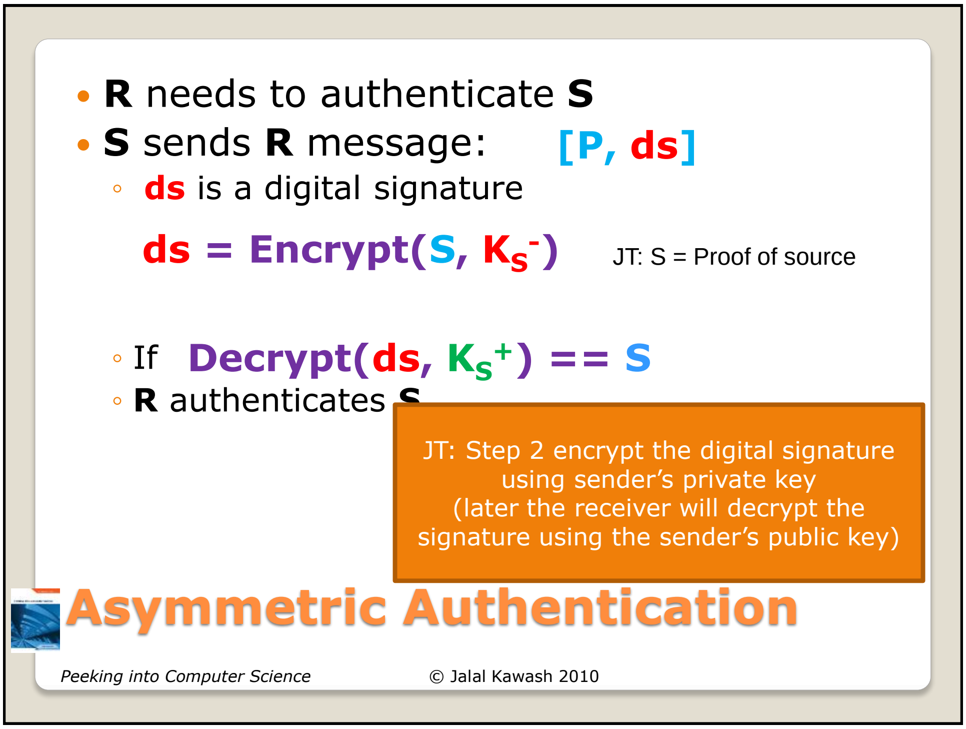
This is Tam’s secret message

- Step 1: Encrypt message (no one read or modify the message)
    - My computer encrypts message using recipient computer’s public key
- Step 2: Prove the message came from me (protect against phishing fabrication attempts)
    - My computer encrypts a digital signature using a private key
    - The recipient computer uses a corresponding public key to view the digital signature.



JT: Authentication In Practice (3)

- My computer is the only one can encrypt the digital signature with that private key
- Properly implemented digital signatures are more difficult to forge than a handwritten signature.



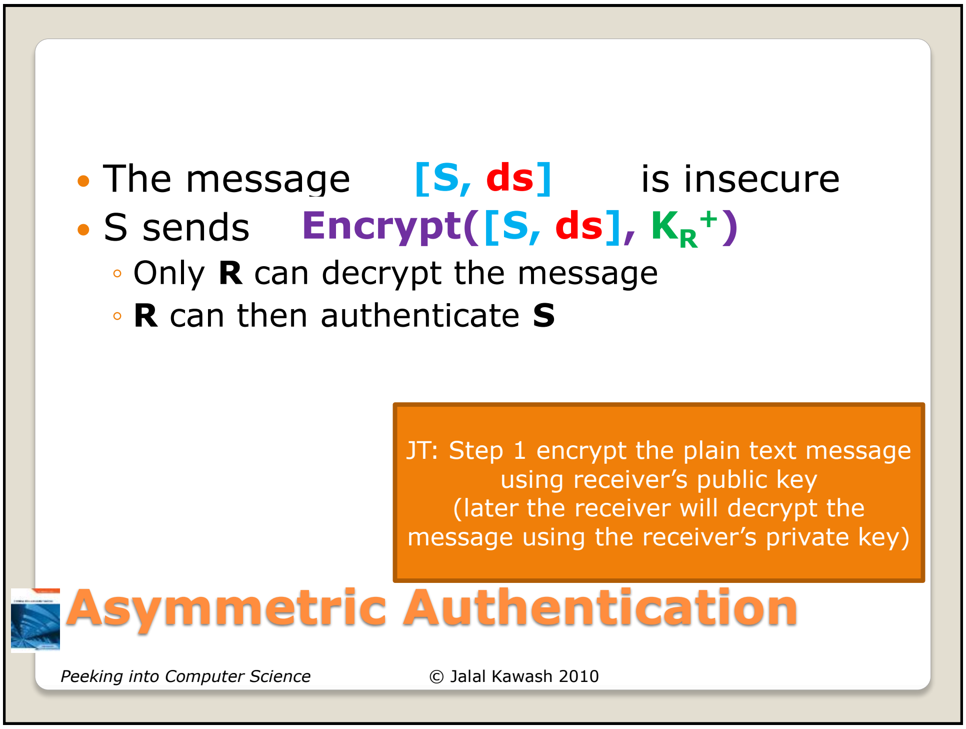
Asymmetric Authentication

- **R** needs to authenticate **S**
- **S** sends **R** message: **[P, ds]**
  - **ds** is a digital signature

    $ds = Encrypt(S, K_S^-)$ JT: S = Proof of source

  - If **$Decrypt(ds, K_S^+) == S$**
  - **R** authenticates **S**

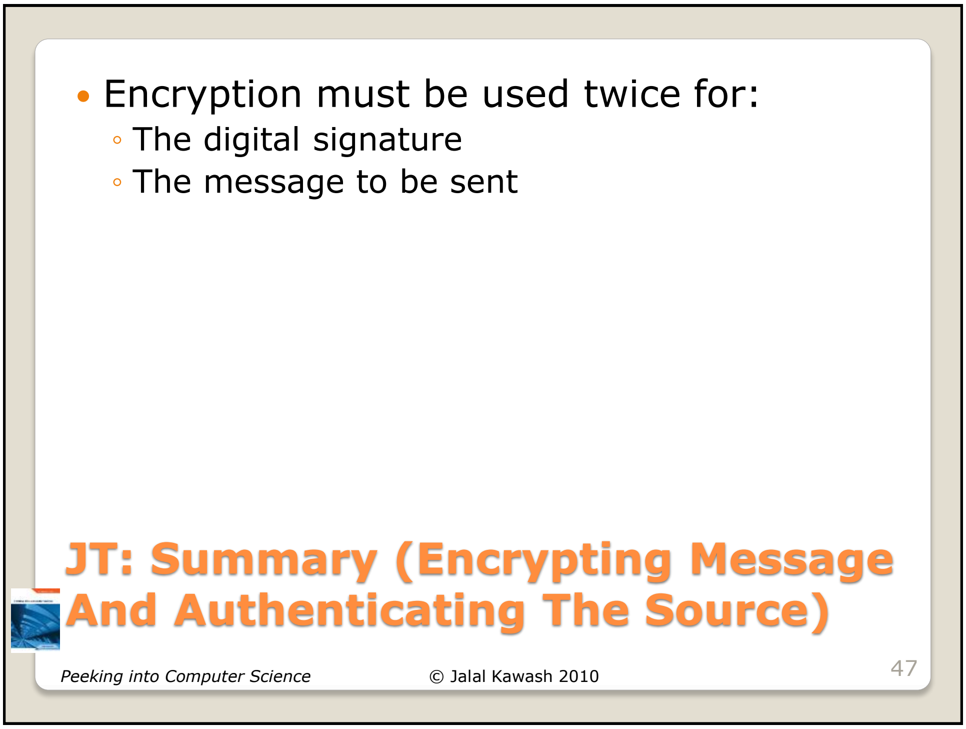
JT: Step 2 encrypt the digital signature using sender's private key (later the receiver will decrypt the signature using the sender's public key)



Asymmetric Authentication

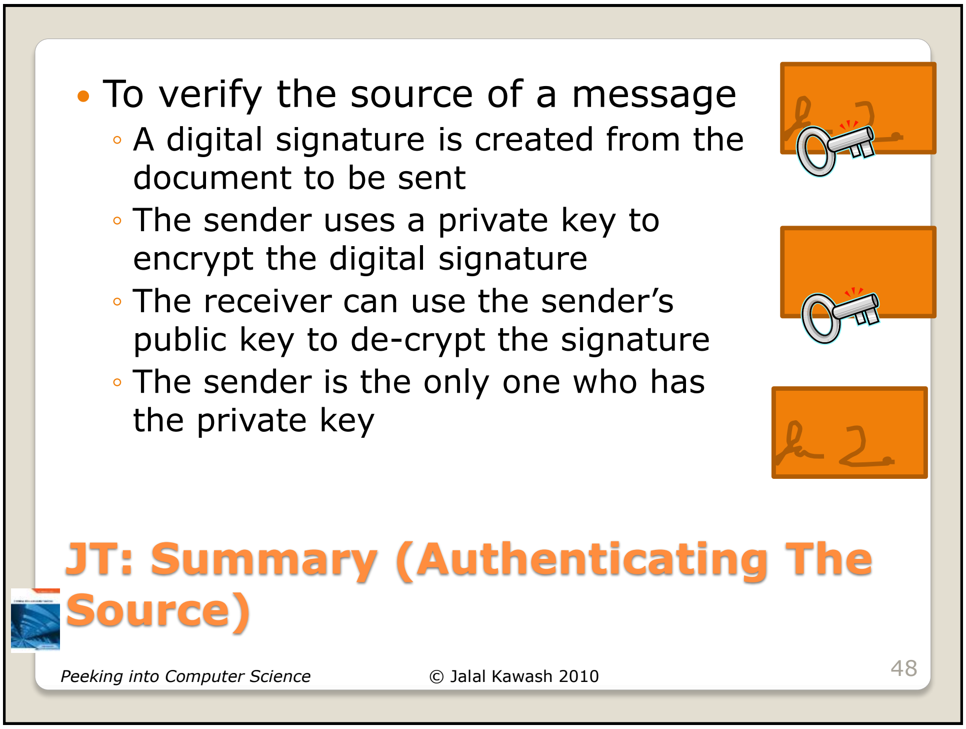
- The message **[S, ds]** is insecure
- S sends **$Encrypt([S, ds], K_R^+)$**
  - Only **R** can decrypt the message
  - **R** can then authenticate **S**

JT: Step 1 encrypt the plain text message using receiver's public key (later the receiver will decrypt the message using the receiver's private key)



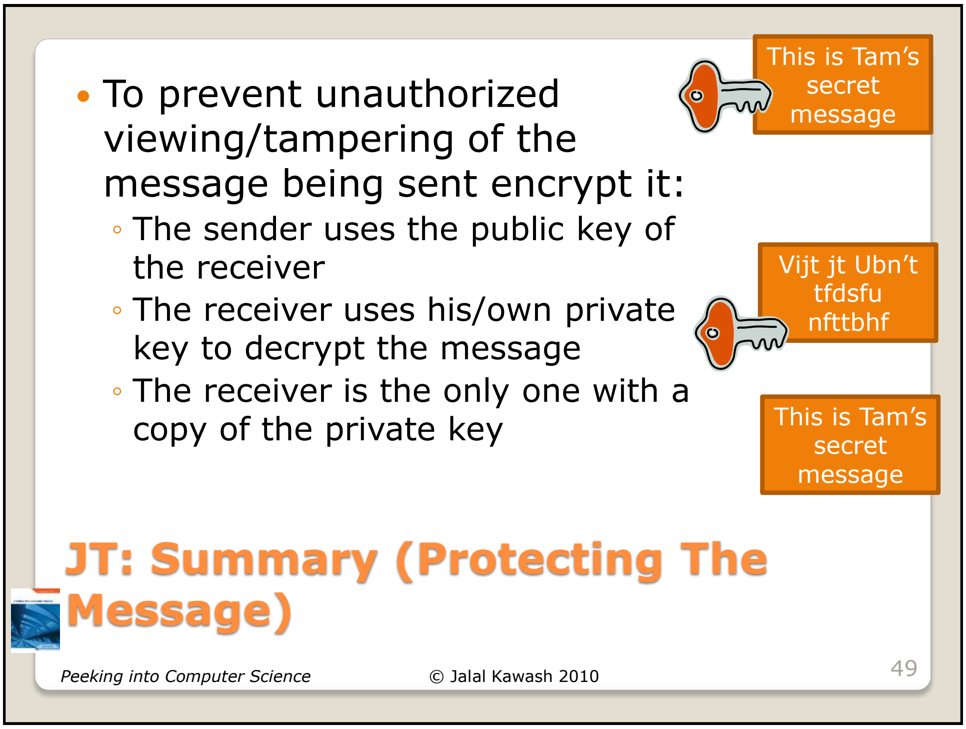
JT: Summary (Encrypting Message And Authenticating The Source)

- Encryption must be used twice for:
  - The digital signature
  - The message to be sent



JT: Summary (Authenticating The Source)

- To verify the source of a message
  - A digital signature is created from the document to be sent
  - The sender uses a private key to encrypt the digital signature
  - The receiver can use the sender’s public key to de-crypt the signature
  - The sender is the only one who has the private key

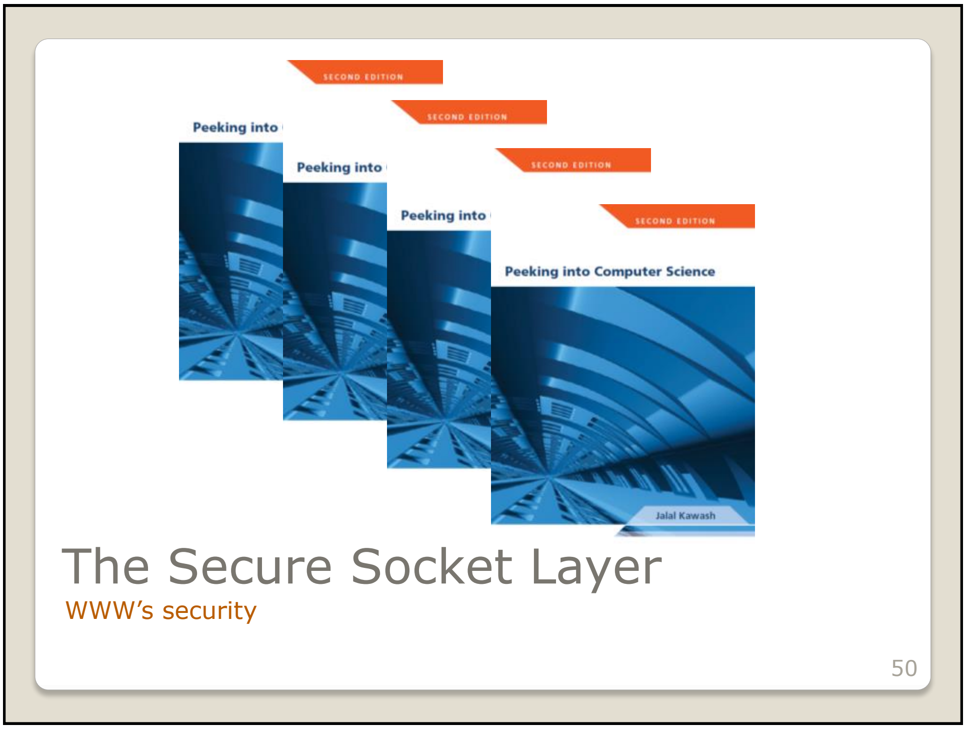


JT: Summary (Protecting The Message)

- To prevent unauthorized viewing/tampering of the message being sent encrypt it:
  - The sender uses the public key of the receiver
  - The receiver uses his/own private key to decrypt the message
  - The receiver is the only one with a copy of the private key

This is Tam's secret message
Vijt jt Ubn't tfdsfu nfttbhf
This is Tam's secret message

Peeking into Computer Science © Jalal Kawash 2010 49

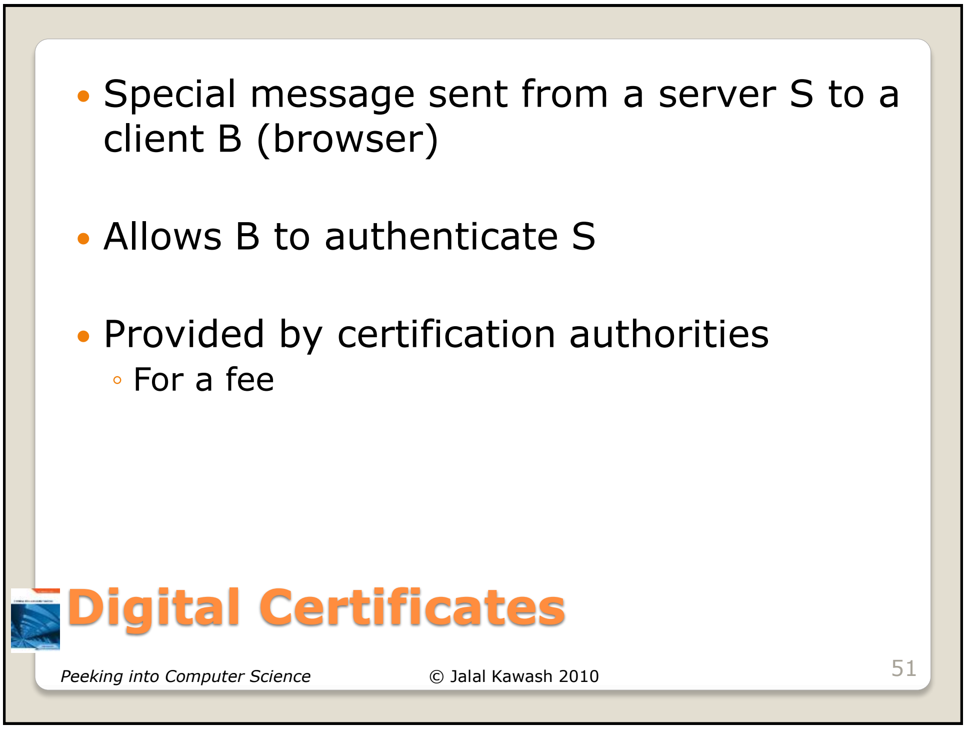


SECOND EDITION
Peeking into Computer Science
Jalal Kawash

The Secure Socket Layer

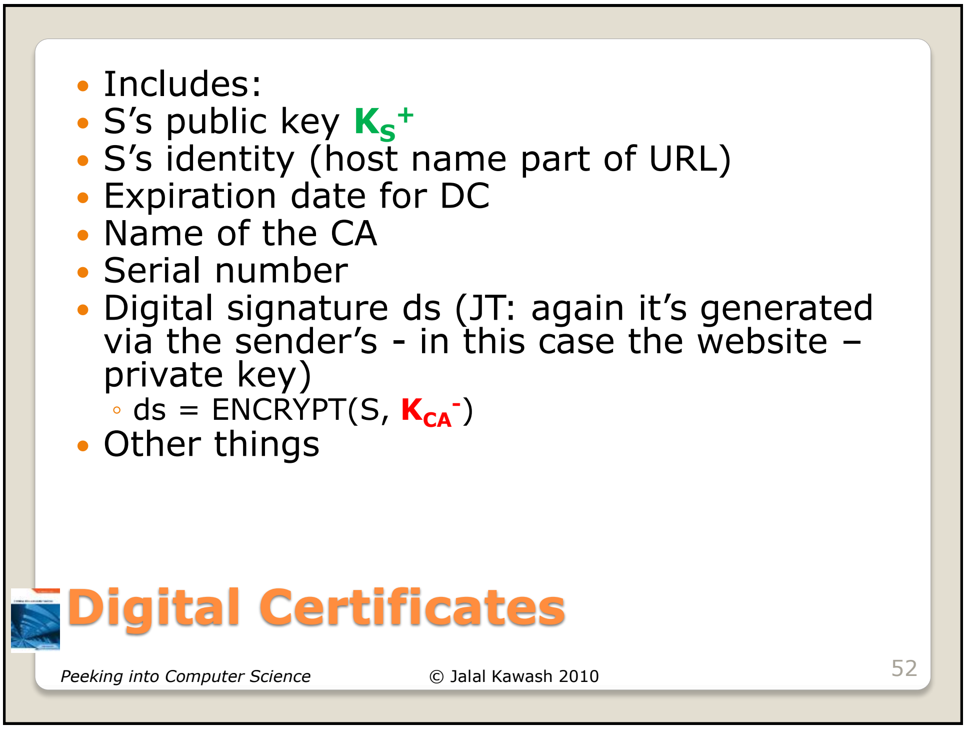
WWW's security

50



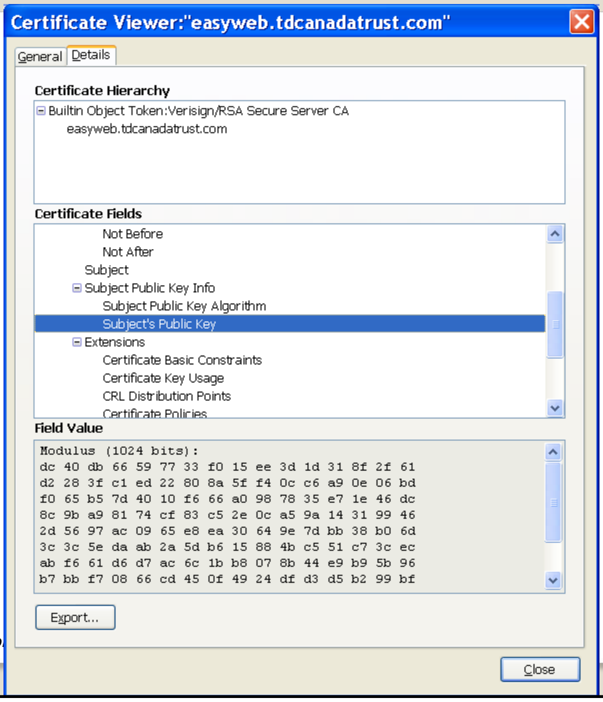
Digital Certificates

- Special message sent from a server S to a client B (browser)
- Allows B to authenticate S
- Provided by certification authorities
  - For a fee



Digital Certificates

- Includes:
- S’s public key K_S^+
- S’s identity (host name part of URL)
- Expiration date for DC
- Name of the CA
- Serial number
- Digital signature ds (JT: again it’s generated via the sender’s - in this case the website – private key)
  - ds = ENCRYPT(S, K_{CA}^-)
- Other things



Certificate Viewer:"easyweb.tdcanadatrust.com"

Certificate Hierarchy

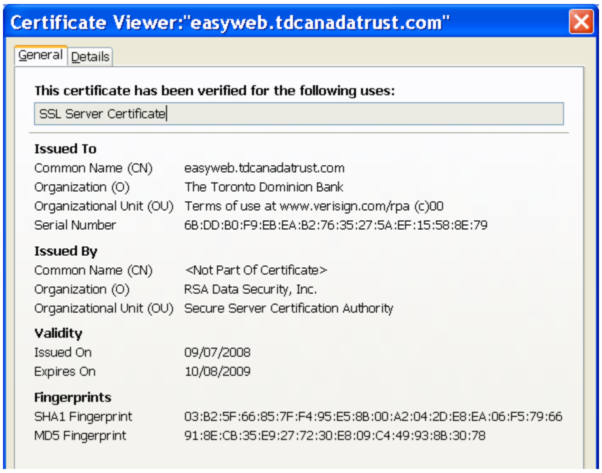
- Builtin Object Token:Verisign/RSA Secure Server CA
  - easyweb.tdcanadatrust.com

Certificate Fields

```
        Not Before
        Not After
     Subject
   ⊟ Subject Public Key Info
        Subject Public Key Algorithm
        Subject's Public Key
   ⊟ Extensions
        Certificate Basic Constraints
        Certificate Key Usage
        CRL Distribution Points
        Certificate Policies
```

Field Value

```
Modulus (1024 bits):
dc 40 db 66 59 77 33 f0 15 ee 3d 1d 31 8f 2f 61
d2 28 3f c1 ed 22 80 8a 5f f4 0c c6 a9 0e 06 bd
f0 65 b5 7d 40 10 f6 66 a0 98 78 35 e7 1e 46 dc
8c 9b a9 81 74 cf 83 c5 2e 0c a5 9a 14 31 99 46
2d 56 97 ac 09 65 e8 ea 30 64 9e 7d bb 38 b0 6d
3c 3c 5e da ab 2a 5d b6 15 88 4b c5 51 c7 3c ec
ab f6 61 d6 d7 ac 6c 1b b8 07 8b 44 e9 b9 5b 96
b7 bb f7 08 66 cd 45 0f 49 24 df d3 d5 b2 99 bf
```



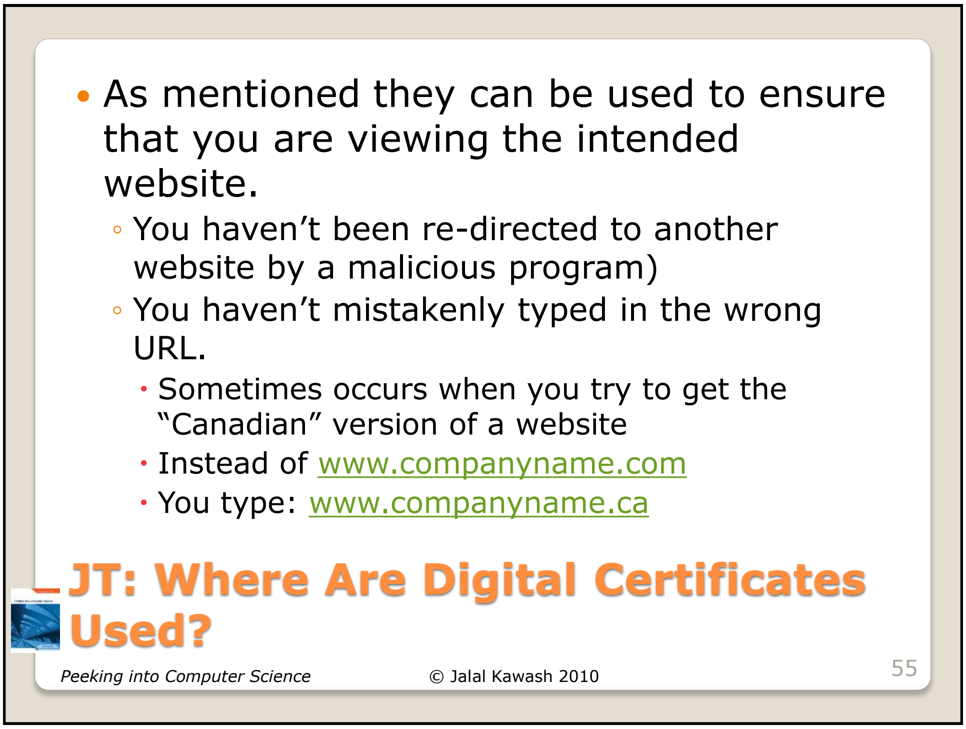
Certificate Viewer:"easyweb.tdcanadatrust.com"

This certificate has been verified for the following uses:

SSL Server Certificate

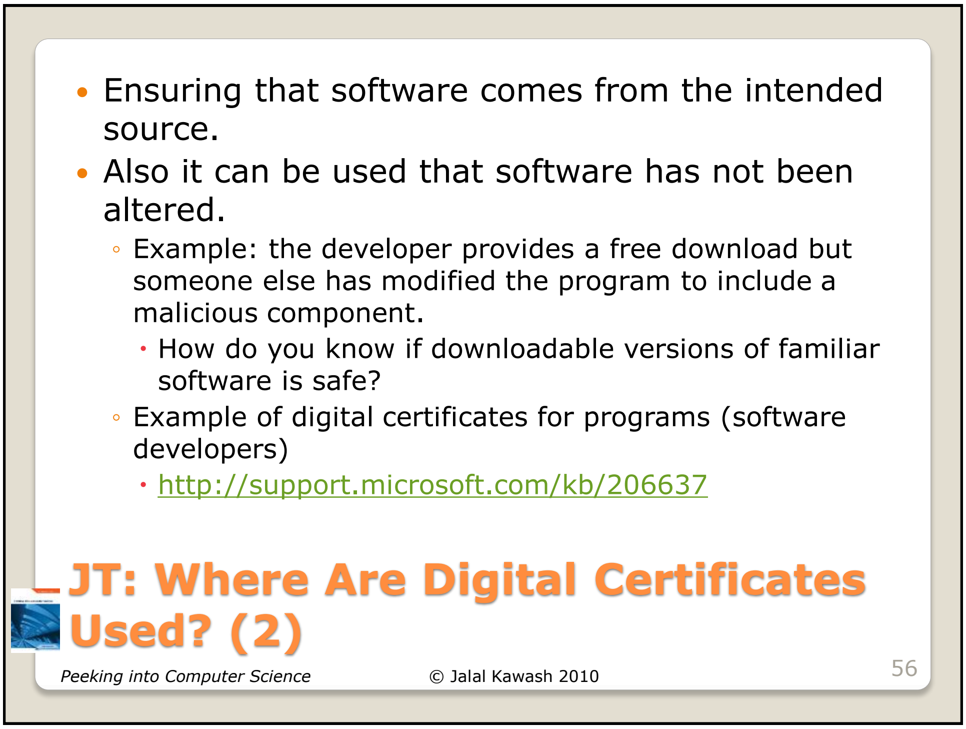
Issued To	
Common Name (CN)	easyweb.tdcanadatrust.com
Organization (O)	The Toronto Dominion Bank
Organizational Unit (OU)	Terms of use at www.verisign.com/rpa (c)00
Serial Number	6B:DD:B0:F9:EB:EA:B2:76:35:27:5A:EF:15:58:8E:79
Issued By	
Common Name (CN)	<Not Part Of Certificate>
Organization (O)	RSA Data Security, Inc.
Organizational Unit (OU)	Secure Server Certification Authority
Validity	
Issued On	09/07/2008
Expires On	10/08/2009
Fingerprints	
SHA1 Fingerprint	03:B2:5F:66:85:7F:F4:95:E5:8B:00:A2:04:2D:E8:EA:06:F5:79:66
MD5 Fingerprint	91:8E:CB:35:E9:27:72:30:E8:09:C4:49:93:8B:30:78

Viewing a DS in FireFox



JT: Where Are Digital Certificates Used?

- As mentioned they can be used to ensure that you are viewing the intended website.
  - You haven't been re-directed to another website by a malicious program)
  - You haven't mistakenly typed in the wrong URL.
    - Sometimes occurs when you try to get the "Canadian" version of a website
    - Instead of www.companyname.com
    - You type: www.companyname.ca



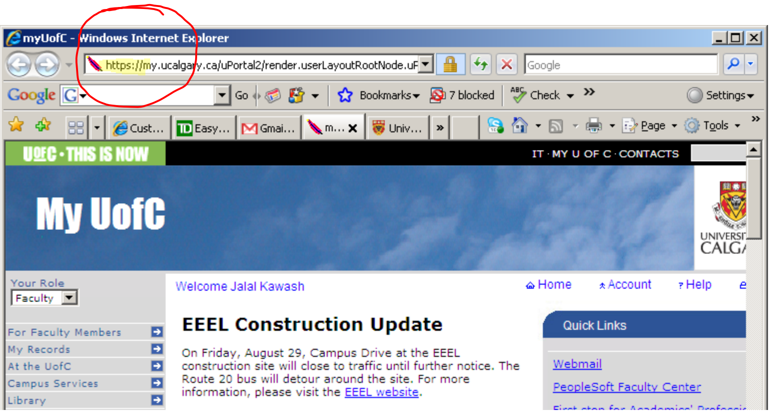
JT: Where Are Digital Certificates Used? (2)

- Ensuring that software comes from the intended source.
- Also it can be used that software has not been altered.
  - Example: the developer provides a free download but someone else has modified the program to include a malicious component.
    - How do you know if downloadable versions of familiar software is safe?
  - Example of digital certificates for programs (software developers)
    - http://support.microsoft.com/kb/206637

Secure Socket Layer (SSL)

- Turned on by HTTP**S**
- Browser and server establish secure channel
- Browser authenticates server
  - Uses digital certificate

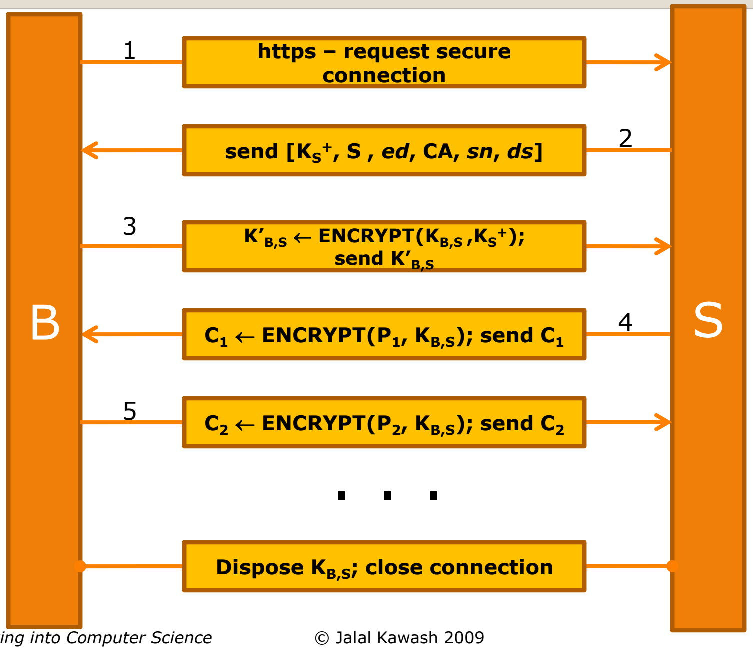
HTTP**S**



Welcome Jalal Kawash

EEEL Construction Update

On Friday, August 29, Campus Drive at the EEEL construction site will close to traffic until further notice. The Route 20 bus will detour around the site. For more information, please visit the EEEL website.



1 https – request secure connection

2 send [K_S^+, S , *ed*, CA, *sn*, *ds*]

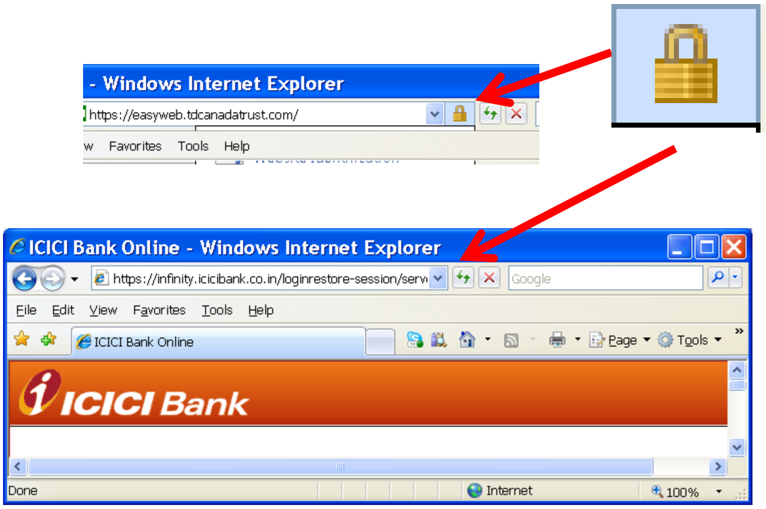
3 $K'_{B,S} \leftarrow$ ENCRYPT($K_{B,S}$,K_S^+); send $K'_{B,S}$

4 $C_1 \leftarrow$ ENCRYPT(P_1, $K_{B,S}$); send C_1

5 $C_2 \leftarrow$ ENCRYPT(P_2, $K_{B,S}$); send C_2

. . .

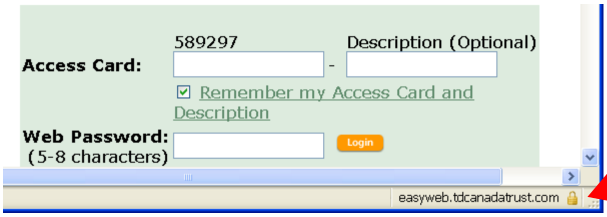
Dispose $K_{B,S}$; close connection


- Windows Internet Explorer
w Favorites Tools Help
ICICI Bank Online - Windows Internet Explorer
Google
File Edit View Favorites Tools Help
ICICI Bank Online
Page
Tools
ICICI Bank
Done
Internet
100%

https://easyweb.tdcanadatrust.com/

https://infinity.icicibank.co.in/loginrestore-session/serv

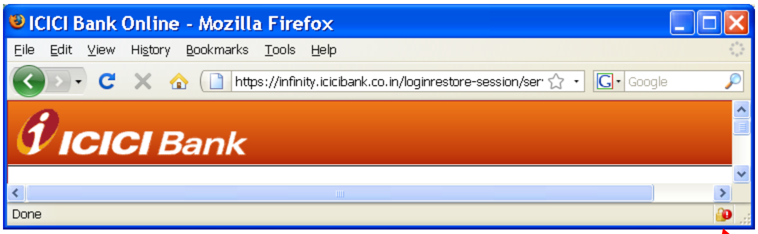
Internet Explorer



Access Card: 589297 - Description (Optional)

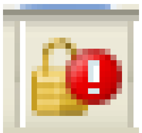
☑ Remember my Access Card and Description

Web Password: (5-8 characters)



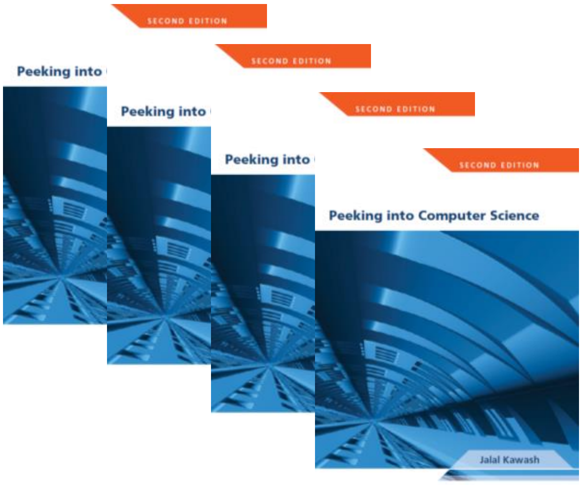
ICICI Bank Online - Mozilla Firefox

https://infinity.icicibank.co.in/loginrestore-session/ser



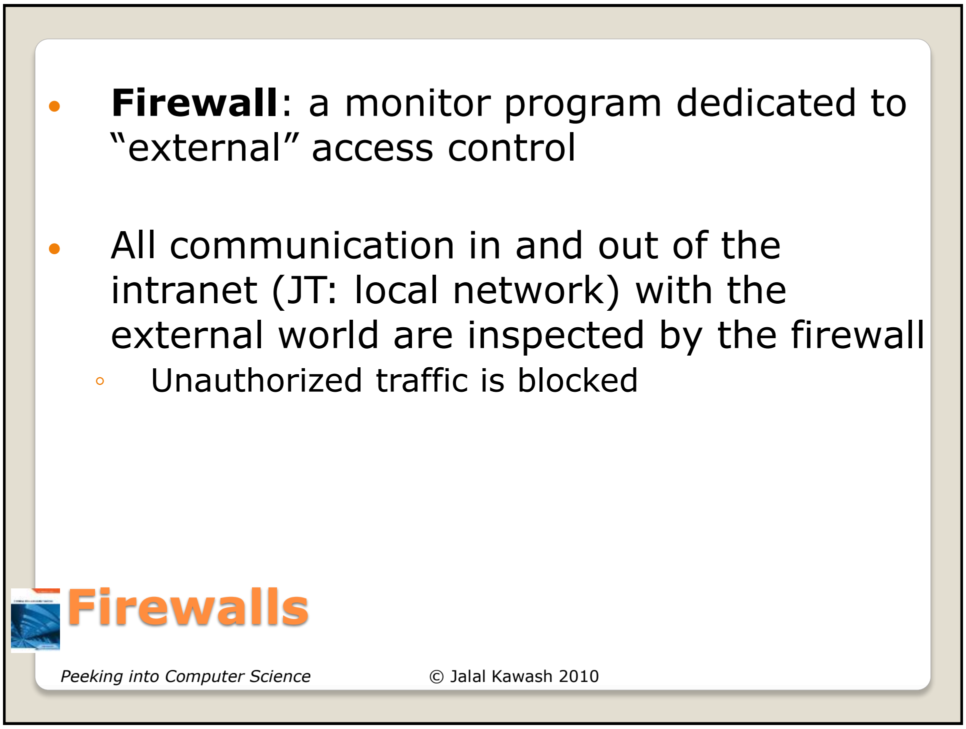
Fire Fox

Peeking into Computer Science © Jalal Kawash 2010



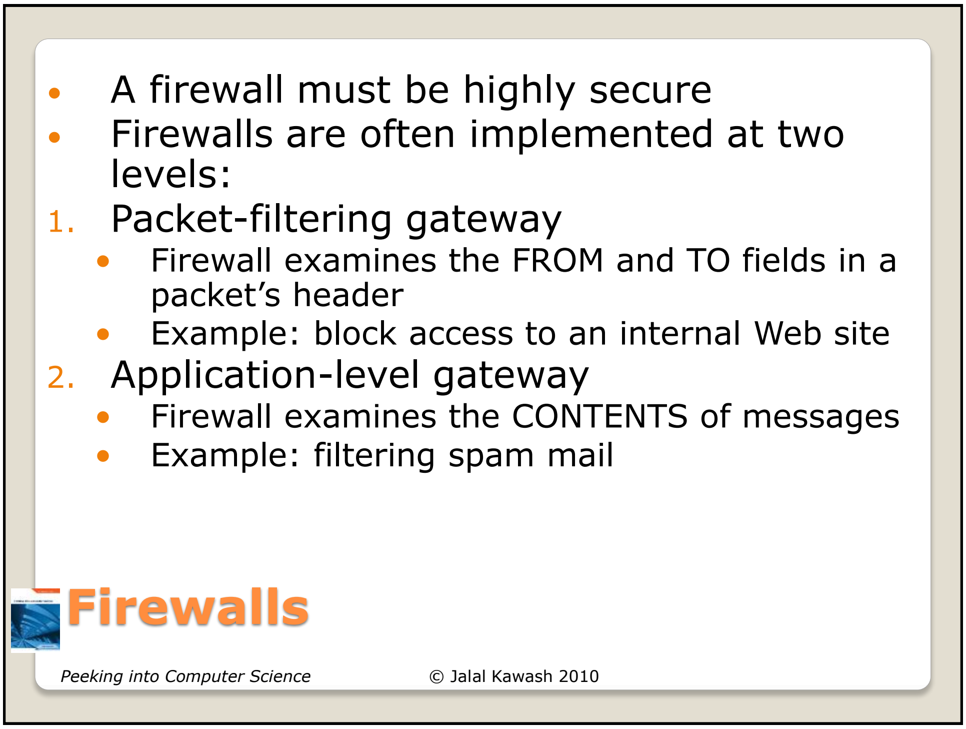
Firewalls

Protect your Computers



Firewalls

- **Firewall**: a monitor program dedicated to "external" access control
- All communication in and out of the intranet (JT: local network) with the external world are inspected by the firewall
  - Unauthorized traffic is blocked



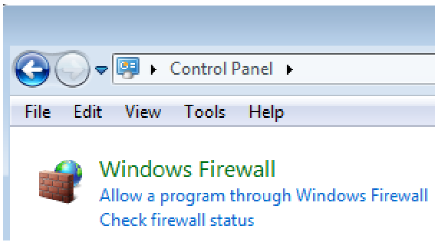
Firewalls

- A firewall must be highly secure
- Firewalls are often implemented at two levels:

1. Packet-filtering gateway
   - Firewall examines the FROM and TO fields in a packet's header
   - Example: block access to an internal Web site
2. Application-level gateway
   - Firewall examines the CONTENTS of messages
   - Example: filtering spam mail

JT: Types Of Firewalls

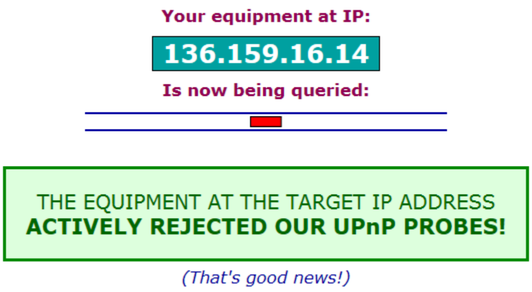
- Firewalls may be included in hardware (built into network routers) or software



JT: Firewalls (Practical Application)

- Firewalls can be used to customize ports
  - Ports that have been maliciously probed from the Internet may be disabled
  - For certain communications non-standard ports may be used instead e.g., UC-IT uses port 465 instead of 110 because many ‘spam’ programs send junk mail using #110.

- Example: “Shields up” https://www.grc.com/x/ne.dll?bh0bkyd2



Your equipment at IP:

136.159.16.14

Is now being queried:

THE EQUIPMENT AT THE TARGET IP ADDRESS
ACTIVELY REJECTED OUR UPnP PROBES!

(That's good news!)

JT: Evaluating The Security Of Your Connection