Network Security

COS 460 & 540

HOMELAND SECURITY ADVISORY SYSTEM

DANGER DOG

SEVERE RISK OF TERRORIST ATTACKS

CHICAGO DOG

HIGH RISK OF TERRORIST ATTACKS

KOSHER DOG

SIGNIFICANT RISK OF TERRORIST ATTACKS

WIENER

GENERAL RISK OF TERRORIST ATTACKS

TOFU PUP

LOW RISK OF TERRORIST ATTACKS

Threat Types

- Data *integrity* and *confidentiality*
- Endpoint *trust* and *access*
- Denial of *service*
- *D*enial of *activity*

Confidentiality

Confidentiality means a third-party cannot eavesdrop on the communication.

Confidentiality

Traffic o one can tell th d.

Confidentiality

Encr

Data Integrity

"CRC and checksum values already protect my data."

Checksum & CRC

CRC and checksum do not tell who sent the data, only that it “looks right”

Data Integrity

- Tampering
- Replay Attacks
- Originality
- Delay (timeliness)

Tampering

"I only ordered one Tribble"

Replay Attack

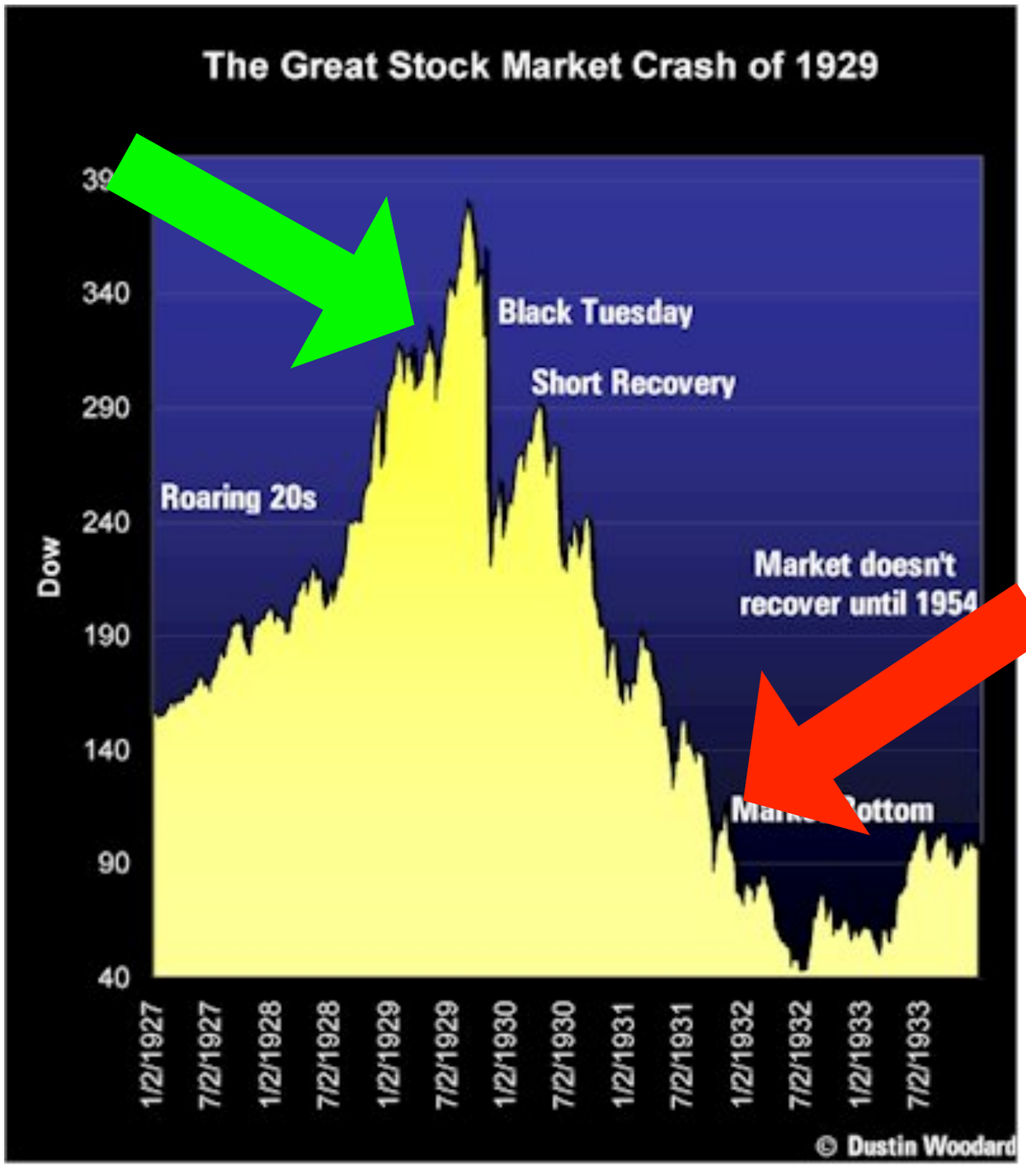
Replay Attack

```
Username:  fred

Password:  lisa

8
```

Delay


The Great Stock Market Crash of 1929
Black Tuesday
Short Recovery
Roaring 20s
Market doesn't
recover until 1954
Dow
340
290
240
190
140
90
40
1/2/1927
7/2/1927
1/2/1928
7/2/1928
1/2/1929
7/2/1929
1/2/1930
7/2/1930
1/2/1931
7/2/1931
1/2/1932
7/2/1932
1/2/1933
7/2/1933
© Dustin Woodard

Denial of Service

Denial of Activity

"These aren't the droids you're looking for."

Threat Types

- Data *integrity* and *confidentiality*
- Endpoint *trust* and *access*
- Denial of *service*
- *D*enial of *activity*

Security Tools

- Authentication & Authorization (OS)
- Cryptography
- Firewalls

Authentication

Access Control (Authorization)

Cryptography Tools

- Ciphers
- Hashes
- Key Distribution

Ciphers

- plaintext - the message
- cipher - function that *encrypts*
- ciphertext - the encoded message

Cipher

Hello

World

Axeeh

Phkew

Ciphers

- Symmetric-key
- Asymmetric-key

Symmetric Key

- "Key" shared by all parties
- "Key" used for encryption and decryption

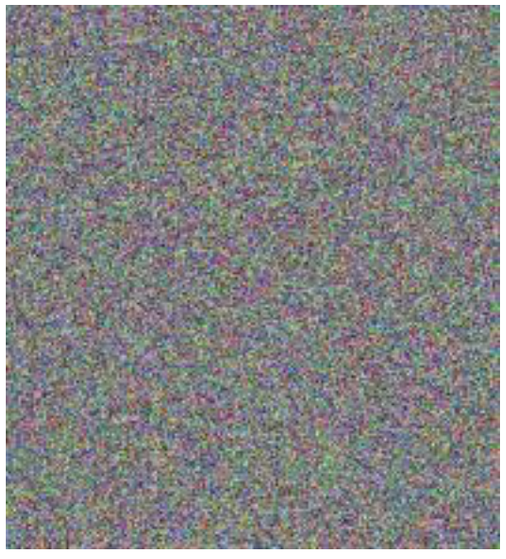
- How do you share the key?
- How do you recover from a lost/stolen key

Exclusive OR

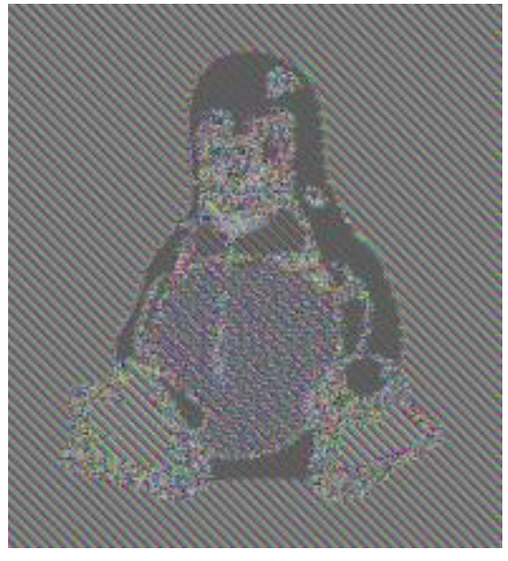
message	0	1	1	0	0	1	1	1
key	1	1	1	1	0	0	0	0
cipherT	1	0	0	1	0	1	1	1
key	1	1	1	1	0	0	0	0
message	0	1	1	0	0	1	1	1

The Problem

Original



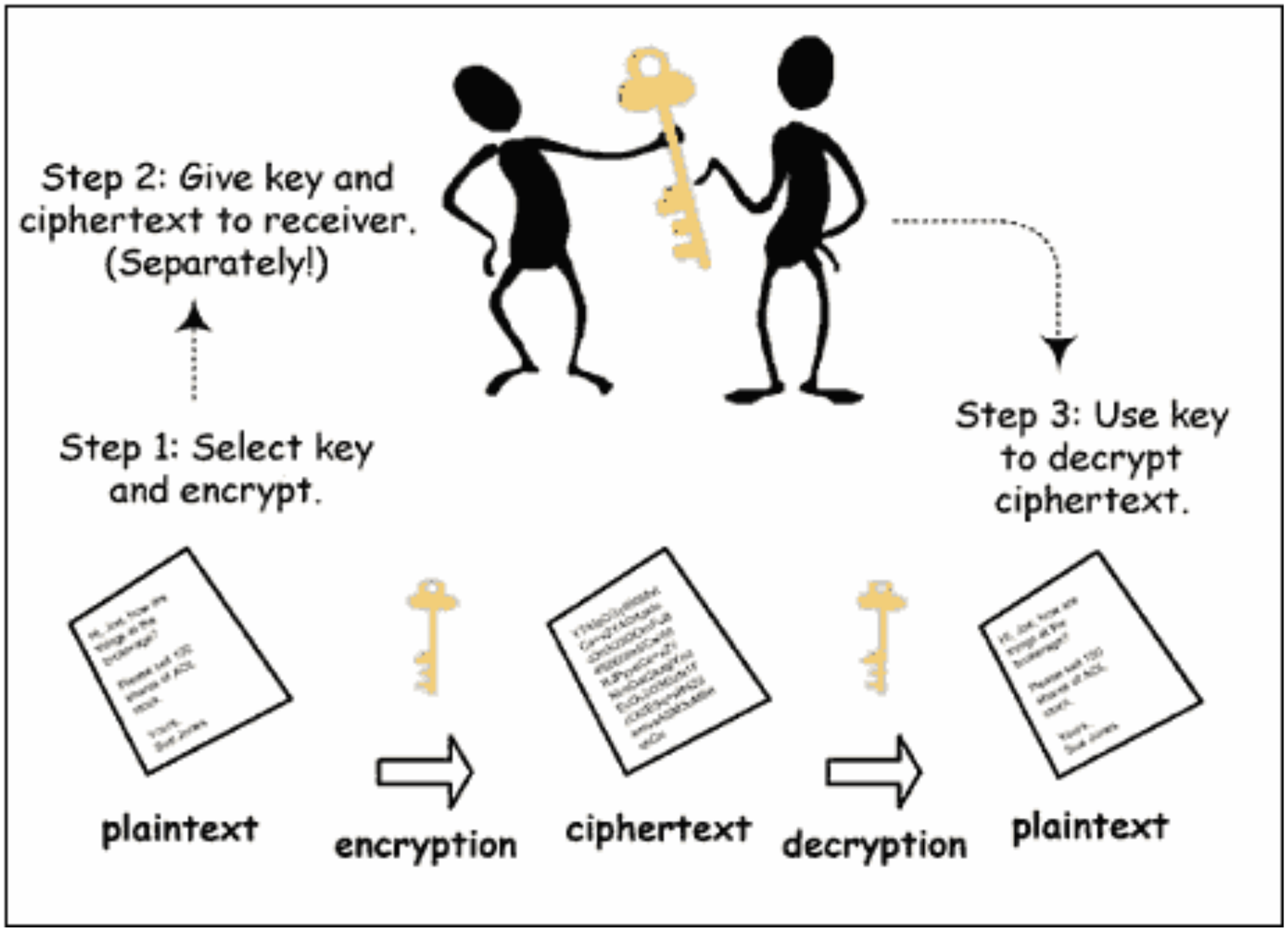
What we “want”



Reality

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Symmetric Key



Key: A=T

Hello

World

Axeeh

Phkew

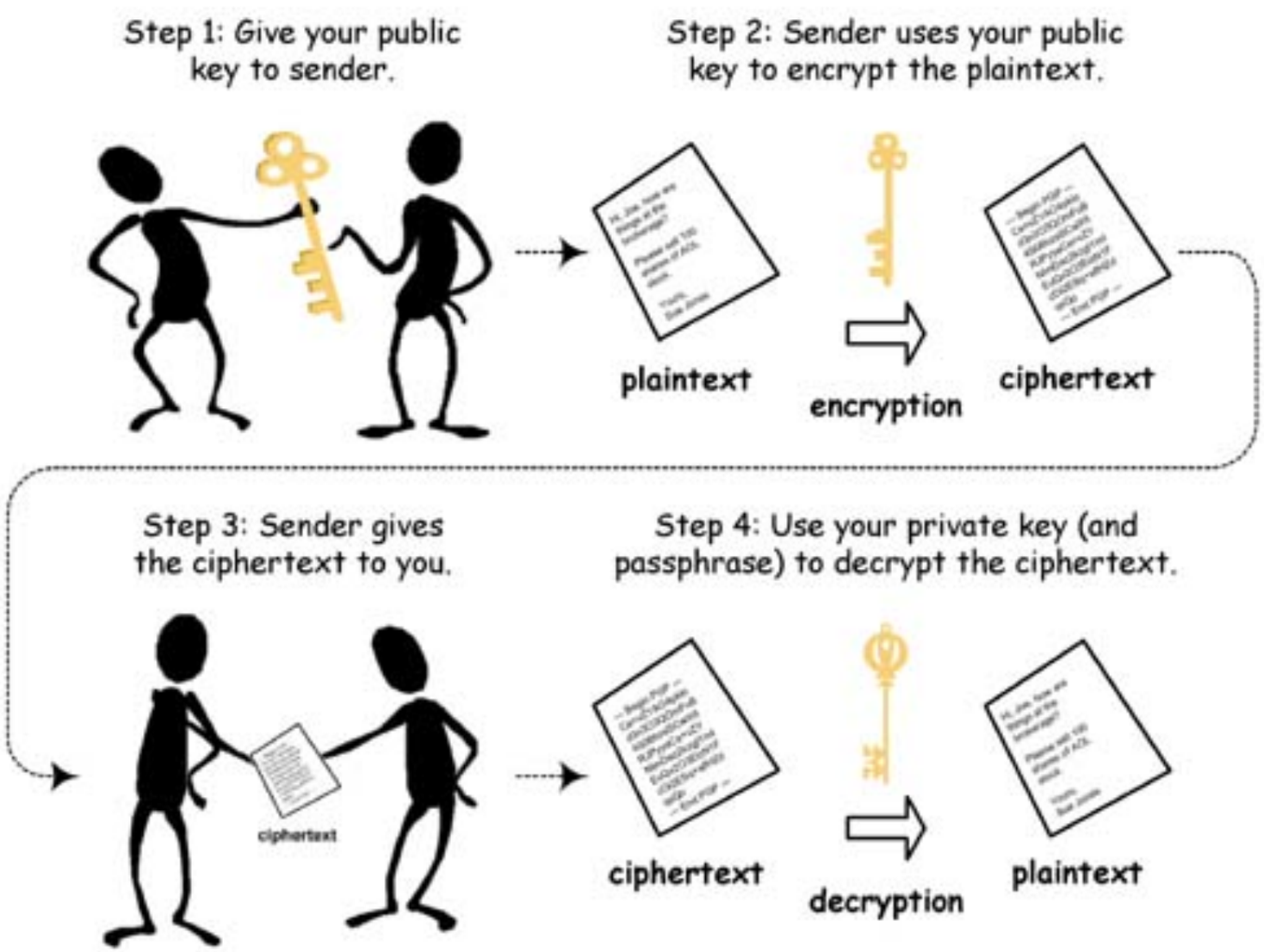
Symmetric Key

- Example: Data Encryption Standard (DES)
  - 56 bit key
  - also, Triple DES = DES x 3
  - is running same encryption 3x better?
- Advanced Encryption Standard (AES)
  - 128, 192, 256 bits in key

Asymmetric Key

- Also known as Public Key Ciphers
- Two “keys”
  - Encryption (private)
  - Decryption (public)
- Share decryption key freely

Asymmetric Key



Asymmetric Keys

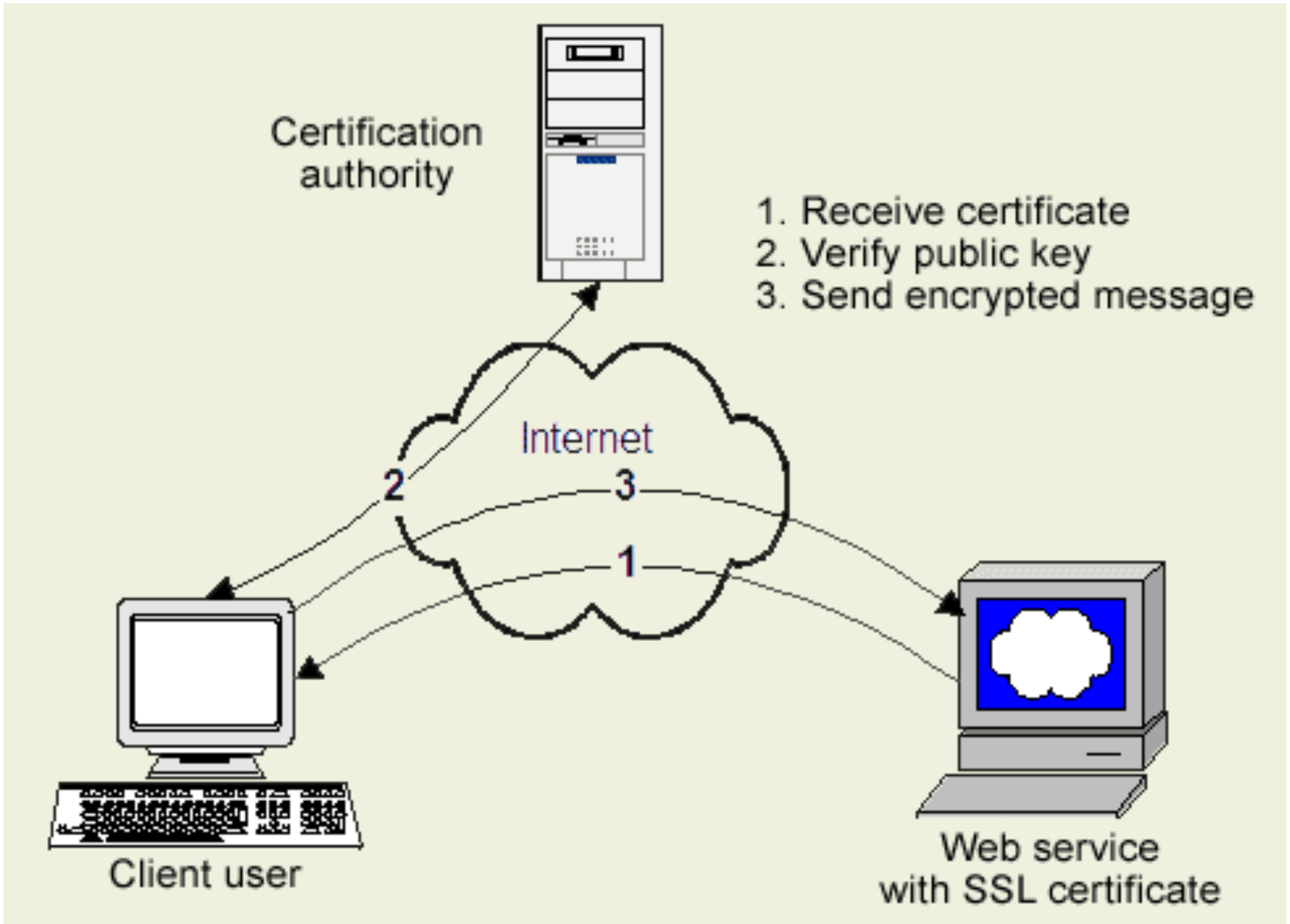
- What's the difference between public and private keys?

- Use public key to encrypt so only private key can decrypt.

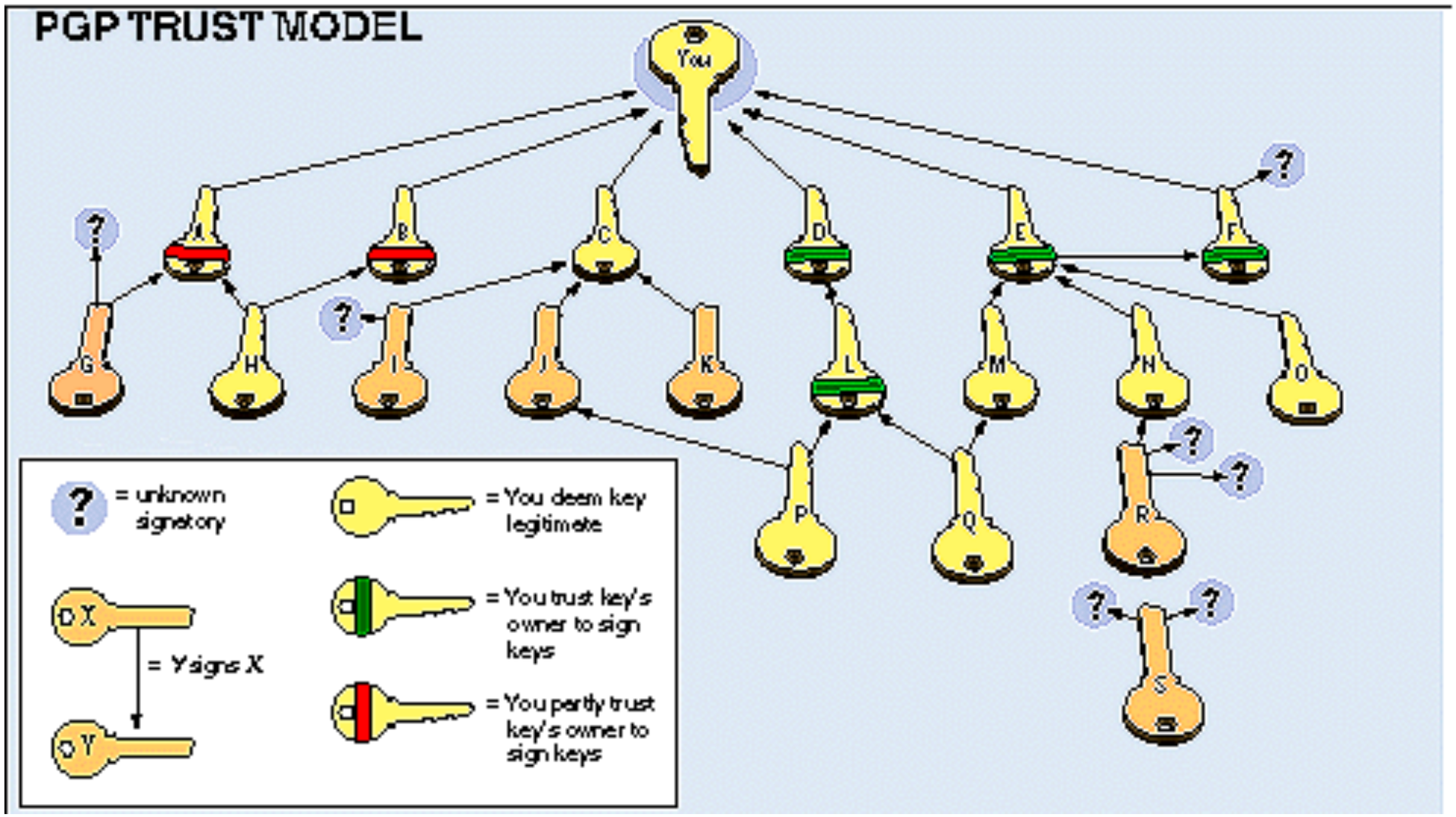
Public-Key Distribution

We need a method to reliably get public-keys so we can reliably decrypt messages.

Certificate Authority



Web of Trust


PGP TRUST MODEL
You
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
?
= unknown signatory
= You deem key legitimate
= You trust key's owner to sign keys
= You partly trust key's owner to sign keys
X
= Y signs X
Y

Asymmetric Keys

- Other Benefits
  - Authentication of sender
  - Limit reception to one receiver
- Problems
  - Public key distribution (validation of)
  - Complexity = slow

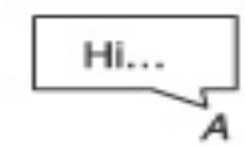
Authenticators

- "digest" or "hash" of message
- similar to Checksum or CRC - one way
- High probability sent and received messages are the same.

- Digital Signature = digest encrypted with public-key algorithm

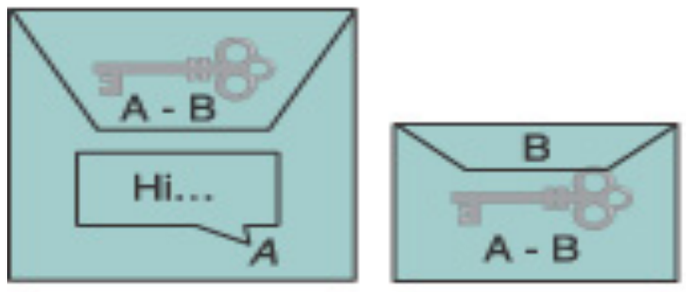
Example: PGP

Hi…= The plaintext message

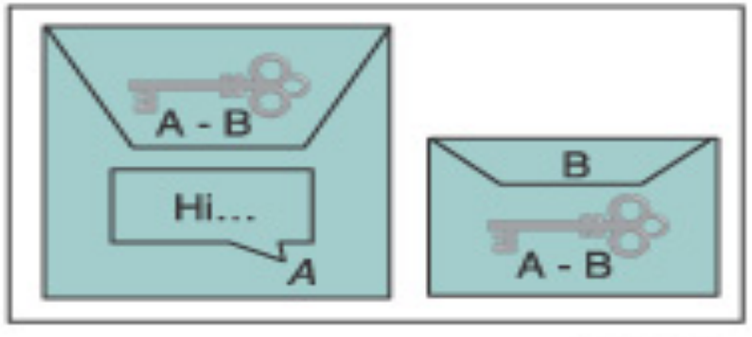


1) Digitally sign
using Alice's private key

2) Encrypt using a newly
generated one-time session key



3) Encrypt the session key using
Bob's public key, and append
that

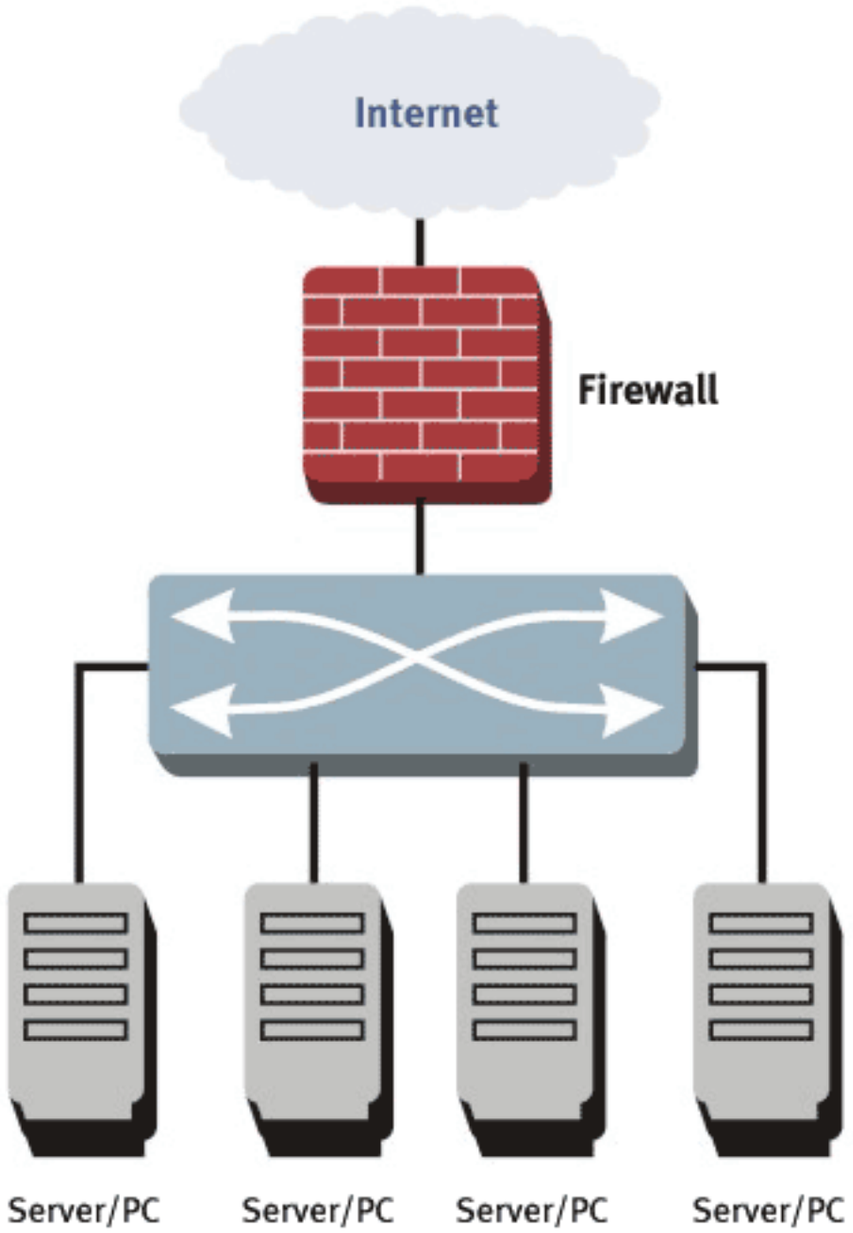


base64

4) Use base64 encoding to
obtain an ASCII-compatible
representation

Firewalls

- "Zones" of trust
  - Internal
  - DMZ
  - Internet
- Network Address Tran



Firewalls

- Protects from undesirable traffic
- Can be deployed by one user
  - no endpoint agreement needed
- Once "inside" all bets are off
- No protection from "trojans"

Network Security

- Threat types
- Security Tools
  - Cryptography
  - Firewalls

End

Network Security