Tutorial - 9
Network Security

Manohar Kuse
mpkuse@ust.hk
http://ihome.ust.hk/~mpkuse

Ever Wondered?

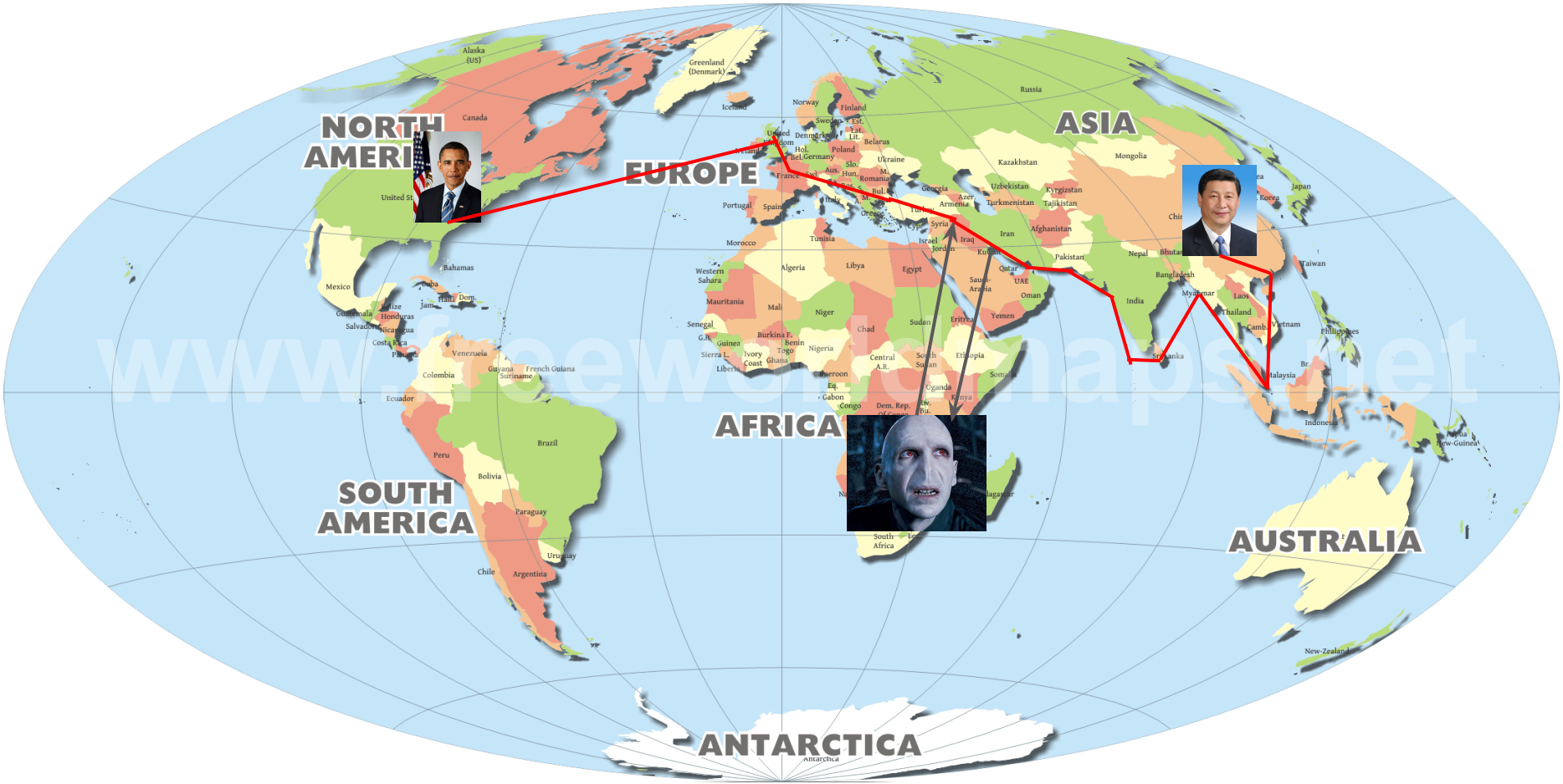
Mr. Xi Jinping (President of PRC)

wants to talk to

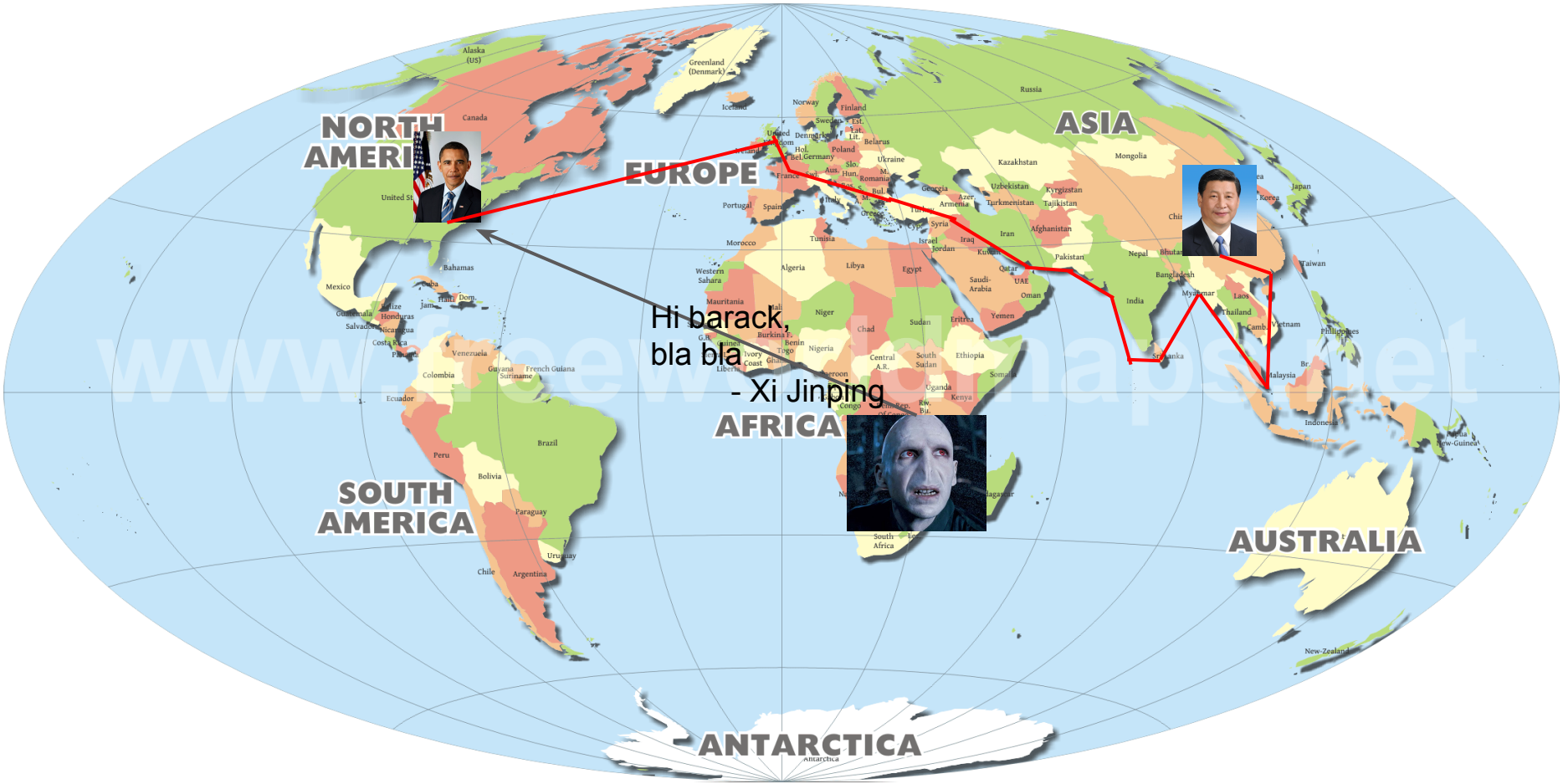
Mr. Barack Obama (President of USA)


NORTH AMERICA
EUROPE
ASIA
AFRICA
SOUTH AMERICA
AUSTRALIA
ANTARCTICA

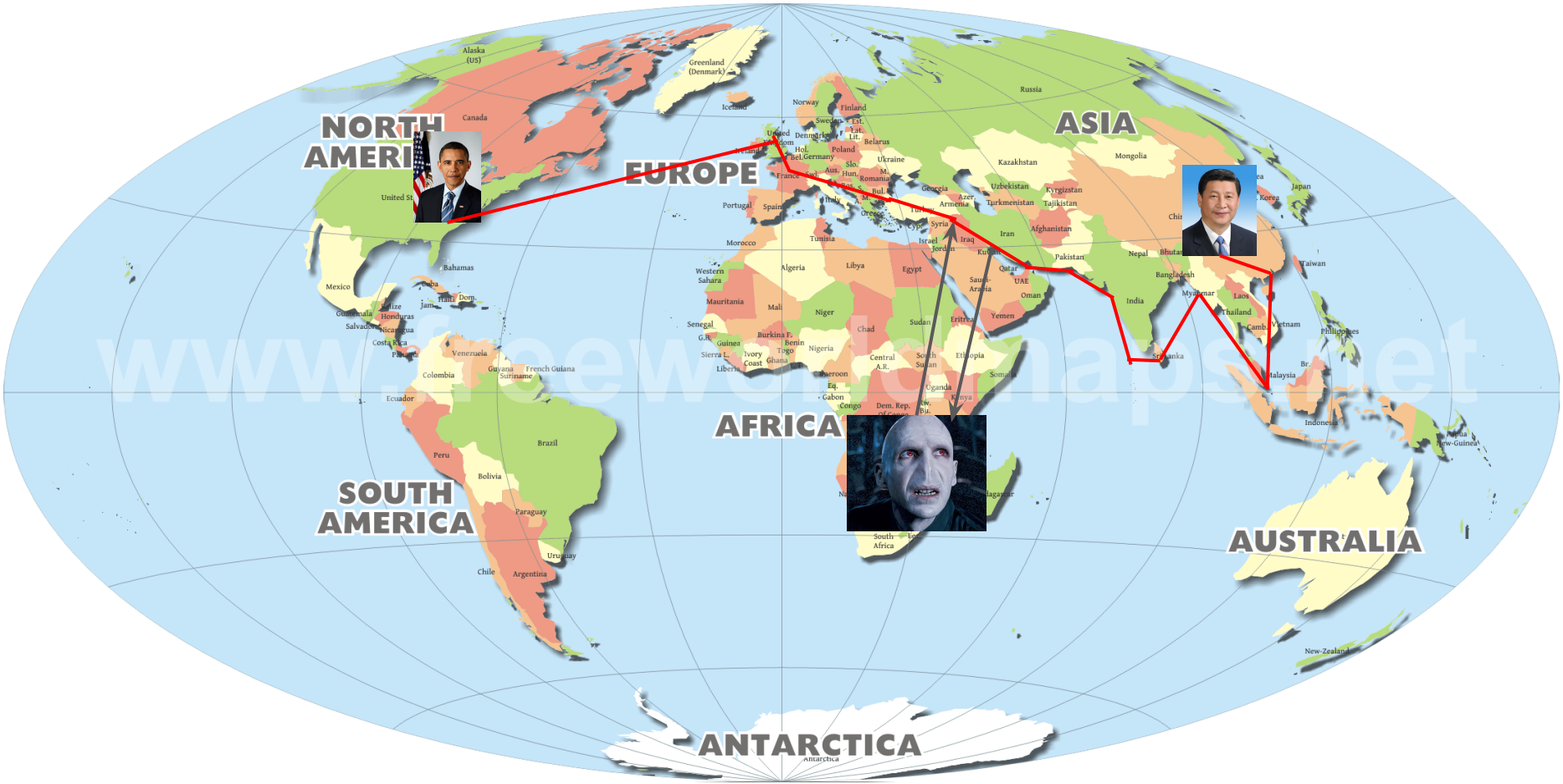
Eavesdropping


NORTH AMERICA
EUROPE
ASIA
AFRICA
SOUTH AMERICA
AUSTRALIA
ANTARCTICA

Insert



Impersonating



Hijack conversation

Denial of service

Attack

- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)
- others

How can they have a private conversation?

Easy answer ⇒ Encrypt the message

May work for : Eavesdropping, Insert,

Does not work for : Impersonation, Hijacking, Denial of service (DoS)

How to Encrypt a Message

Simple Encryption Scheme

Substitution Cipher

Replace A with B

Replace B with C

Replace C with D

.

.

Usage of this cipher

JacK ⇒ KbdL

Terms to Understand

Cipher - The encryption algorithm.

Examples : Substitution cipher, Diffie-Hellman cipher, RSA cipher etc etc.

Plaintext Message - The real info/message that needs to be sent

Key - The secret password with helps to *Decrypt* the message

to 'Encrypt a message' : Plaintext to the coded message using a key

to 'Decrypt a message' : coded message to plaintext using the agreed key

A few more “nice to know” terms

Cryptography - Study of Ciphers

Code breaking - Act of breaking a cipher

Cryptanalysis - Study of cipher breaking

Solved Example - A little complicated cipher

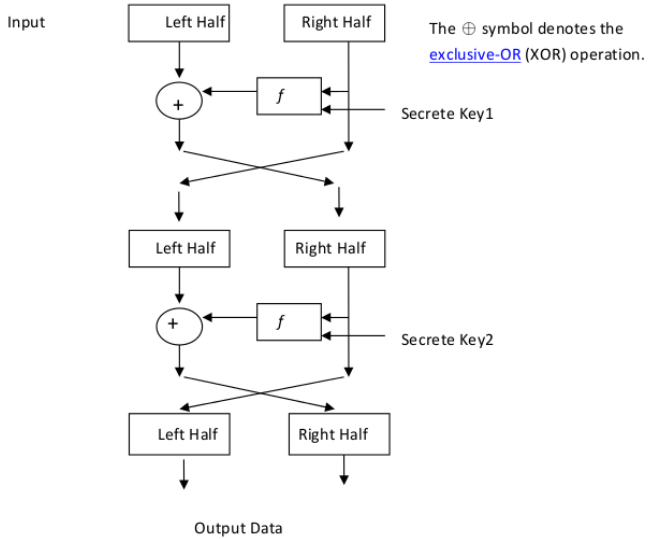
(2) (10 pts) The block diagram of an encryption scheme is shown in the figure below, where *f* has two inputs A and B as shown below:

$$f(A,B) = S(A \oplus B),$$

where $\oplus$ is the XOR operation, and S is a substitution function given below:

0000	->	1100
0001	->	1000
0010	->	0001
0011	->	0010
0100	->	1001
0101	->	0011
0110	->	0001
0111	->	1000
1000	->	0111
1001	->	0000
1010	->	0100
1011	->	0110
1100	->	0101
1101	->	1101
1110	->	1111
1111	->	1110

Assume the block size is 8 bits (left or right half has 4 bits). Key 1 = 1010, Key 2 = 0101 (a) Assume the plaintext is 11000001. Generate the cipher text (b) Repeat (a) for the plaintext 01000001 (see how many bits the two outputs differ).



Categorization of Ciphers

Symmetric Key Cryptography

Public Key Cryptography

Symmetric Key Cryptography

Symmetric Key Cryptography

Password to Encrypt

&

Password to decrypt

are the **same**


NORTH AMERICA
EUROPE
ASIA
AFRICA
SOUTH AMERICA
AUSTRALIA
ANTARCTICA

Public Key Cryptography

What is a ‘Public key’ & ‘Private key’

Each person has 2 set of keys

-1- Public key → Tell this key to everyone

-2- Private key → Only you know this key

RSA Algorithm

There are 2 keys (K1, K2)

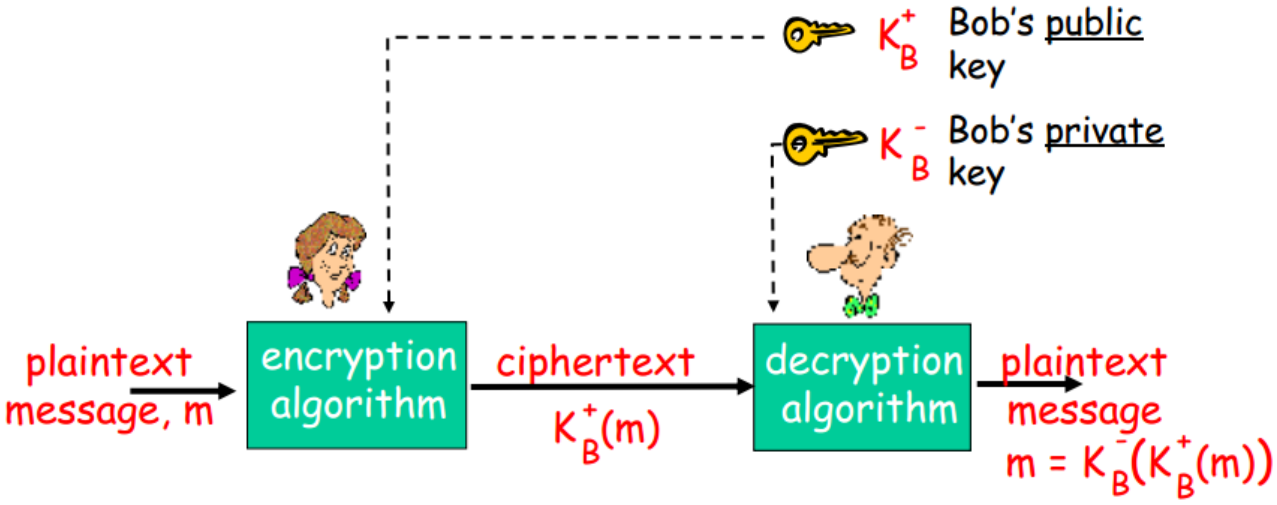
plaintext $\xrightarrow{K1}$ encrypted message $\xrightarrow{K2}$ plaintext

OR

plaintext $\xrightarrow{K2}$ encrypted message $\xrightarrow{K1}$ plaintext

How to perform RSA calculations : http://sergematovic.tripod.com/rsa1.html

How all this plays together?



How to know someone's public key

The person tells it, See :

http://users.stargate.net/~rewilson/PGPClick/mykey.html

http://futureboy.us/pgp.html

http://kusemanohar.wordpress.com/contact-kusemanohar/

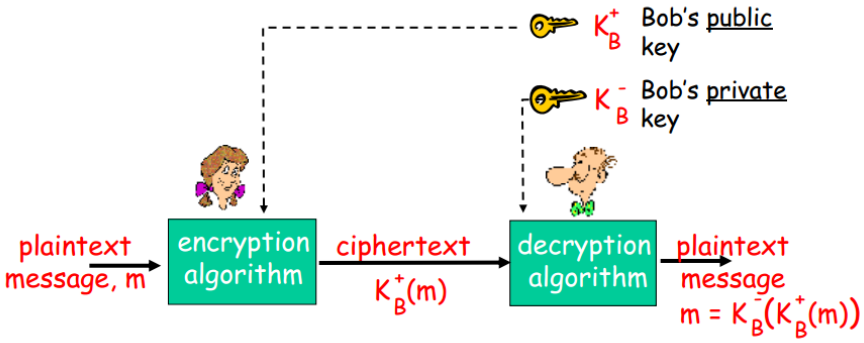
Get it from a trusted key distribution center

eg. Geo Trust Global Inc.

Get yourself a real public & private keys

https://www.igolder.com/pgp/generate-key/

Obama & Xi Jinping



What tools can Obama & XI Jinping use?

Ans: PGP. http://www.pitt.edu/~poole/accessiblePGP703.htm

PGP Tools - Demo

Option 1 :

Follow Tutorial http://www.pitt.edu/~poole/accessiblePGP703.htm

Option 2 :

Use online tool

https://www.igolder.com/pgp/generate-key/

https://www.igolder.com/PGP/encryption/

https://www.igolder.com/PGP/decryption/

Real world considerations

RSA encryption is not practical for all the messages ⇒ RSA has too many computation.

Work around

1. Use RSA to securely communicate a key
2. Once the key is received, encrypt the message with a simple substitution cipher
3. Thus we have different key for each communication we make, hence more secure

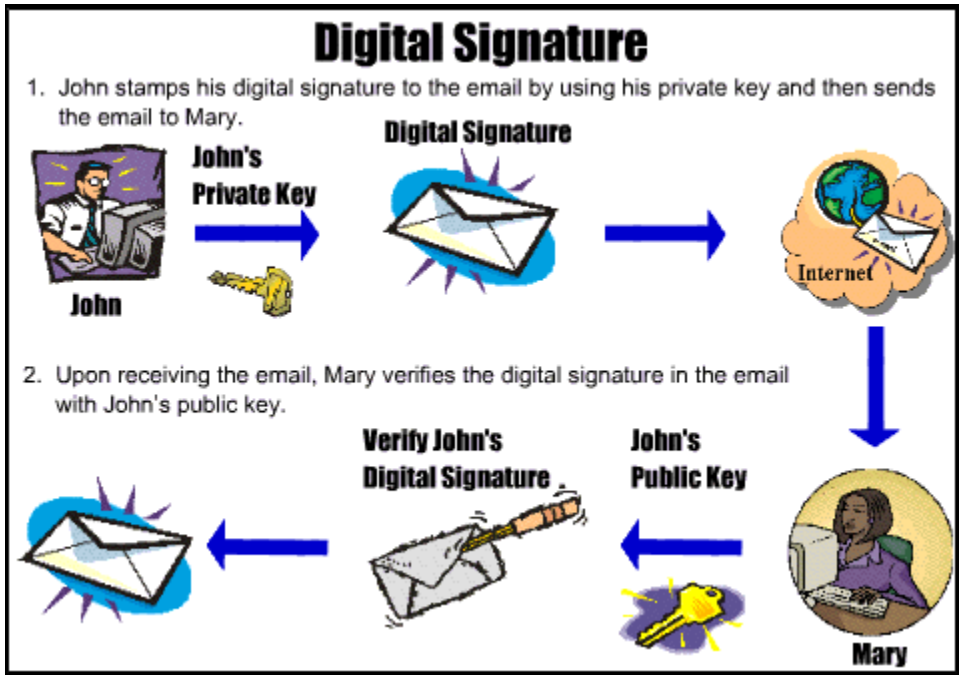
Another trouble

How do we know if the encrypted message is actually coming from the right person?

How to ensure that the message is not sent by a ‘bad guy’?

…..Afterall anyone can send you a message..!

Authenticity of Message - Digital Signature


Digital Signature
1. John stamps his digital signature to the email by using his private key and then sends the email to Mary.
John's
Private Key
Digital Signature
John
Internet
2. Upon receiving the email, Mary verifies the digital signature in the email with John's public key.
Verify John's
Digital Signature
John's
Public Key
Mary

References

PGP Tools - iGolders

https://www.igolder.com/pgp/generate-key/

https://www.igolder.com/PGP/encryption/

https://www.igolder.com/PGP/decryption/

PGP Desktop Tool - tutorial

http://www.pitt.edu/~poole/accessiblePGP703.htm

RSA Algorithm

http://sergematovic.tripod.com/rsa1.html

Other Interesting Links

https://www.youtube.com/watch?v=YEBfamv-_do#t=499

http://futureboy.us/pgp.html