CRYPTOGRAPHY
Secret Key Cryptography

- Single key used to encrypt and decrypt.
- Key must be known by both parties.
- Assuming we live in a hostile environment (otherwise - why the need for cryptography?), it may be hard to share a secret key.
Public Key Cryptography (a.k.a. asymmetric cryptography)

- Relatively new field - 1975 (as far as we know, the NSA is not talking).

- Each entity has 2 keys:
  - private key (a secret)
  - public key (well known).
Using Keys

- Private keys are used for decrypting.
- Public keys are used for encrypting.

plaintext $\rightarrow_{encryption} \text{ciphertext}$

public key $\uparrow$

Ciphertext $\leftarrow_{decryption} \text{plaintext}$

private key $\downarrow$

Netprog: Cryptgraphy
Digital Signature

- Public key cryptography is also used to provide digital signatures.

plaintext → signing → signed message

private key

signed message → verification → plaintext

public key

- Ciphertext

PCQ VMJYPD LBYK LYSO KBXBJXWXV BXV ZCJPO EYPD KBXBJYUXJ LBJOO KCPK. CP LBO LBCMKXPV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: 'DJOXL EYPD, ICJ X LBCMKXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMPLYPD LC UCM LBO IXZROK CI FXKL XDOK XPV LBO RODOPVK CI XPAYOPL EYPDK. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?'

OFYRCDMO, LXROK IJCS LBO LBCMKXPV XPV CPO PYDBLK

Any Guesses???
Frequency Analysis

- Identifying common letters, digrams and trigrams...

  PCQ VMJYPD LBYK LYSO KBXBJXWXXV BXV ZCJPO EYPD KBXBHYUXJ LBJO0 KCPK. CP LBO LBCM KKX PV XPV IYJKL PYDBL, QBOP KBO BXV OPVOV LBO LXRO CI SX'XJMI, KBO JCKO XPV EYKKOV LBO DJCMPV ZOICJO BYS, KXUYPD: 'DJOXL EYPD, X LBCM KXPV XPV CPO PYDBLK Y BXNO ZOOP JOACMP LYPD LC UCM LBO IXZROK CI FKXK XLDOK XPV LBO RODOVK CI XPAYOPL EYPD K. SXU Y SXEO KC ZCRV XK LC AJXNO X IXNCMJ CI UCMJ SXGOKLU?' OFYRCDMO, LXROK IJCS LBO LBCM KXPV XPV CPO PYDBLK

- First guess: LBO is THE
Frequency Analysis

- Assuming **LBO** represents **THE**, we replace **L** with **T**, **B** with **H**, and **O** with **E** and get

- PCQ VMJYPD **THYK TYSE KHXHJXWXV HXV ZCJPE EYPD KHXHJYUXJ THJEE KCPK. CP THE THCMKXPV XPV IYJKT PYDHT, QHEP KHO HXV EPVEV THE LXRE CI SX'XJMI, KHE JCKE XPV EYKKOV THE DJCMPV ZEICJE HYS, KXUYPD: 'DJEXT EYPD, ICJ X LHCMKXPV XPV CPE PYDHLK Y HXNE ZEEP JEACMPTYPD TC UCM THE IXZREK CI FXKL XDEK XPV THE REDEPVK CI XPAYEPT EYPD. SXU Y SXEE KC ZCRV XK TC AJXNE X IXNCMJ CI UCMJ SXGEKTU?'

- More guesses...?
Now during this time Shahrazad had borne King Shahriyar three sons. On the thousand and first night, when she had ended the tale of Ma'aruf, she rose and kissed the ground before him, saying: 'Great King, for a thousand and one nights I have been recounting to you the fables of past ages and the legends of ancient kings. May I make so bold as to crave a favour of your majesty?' Epilogue, Tales from the Thousand and One Nights
Transmitting over an insecure channel.

Alice wants to send Bob a private message.

$A_{\text{public}}$ is Alice’s public key.

$A_{\text{private}}$ is Alice’s private key.

$B_{\text{public}}$ is Bob’s public key.

$B_{\text{private}}$ is Bob’s private key.
Hello Bob,
Wanna get together?

Alice
encrypt using $B_{public}$

Bob
decrypt using $B_{private}$
OK Alice, Your place or mine?

Alice

decrypt using $A_{\text{private}}$

Bob

encrypt using $A_{\text{public}}$
Bob’s Dilemma

- Nobody can read the message from Alice, but anyone could produce it.
- How does Bob know that the message was really sent from Alice?
- Bob may be comforted to know that only Alice can read his reply.
Alice can sign her message!

- Alice can create a digital signature and prove she sent the message (or someone with knowledge of her private key).
- The signature can be a message digest encrypted with $A_{\text{private}}$. 
Message Digest

- Also known as “hash function” or “one-way transformation”.
- Transforms a message of any length and computes a fixed length string.
- We want it to be hard to guess what the message was given only the digest.
  - Guessing is always possible.
Alice’s Signature

- Alice feeds her original message through a hash function and encrypts the message digest with $A_{\text{private}}$.
- Bob can decrypt the message digest using $A_{\text{public}}$.
- Bob can compute the message digest himself.
- If the 2 message digests are identical, Bob knows Alice sent the message.
Revised Scheme

Alice

Sign with $A_{\text{private}}$

encrypt using $B_{\text{public}}$

Bob

check signature using $A_{\text{public}}$

decrypt using $B_{\text{private}}$
Why the digest?

- Alice could just encrypt her name, and then Bob could decrypt it with $A_{public}$.

- Why wouldn’t this be sufficient?
Implications

• Suppose Alice denies she sent the message?

• Bob can prove that only someone with Alice’s key could have produced the message.
Another possible problem

• Suppose Bill receives a message from Alice including a digital signature.
  "its Alice here"

• Bill sends the same message to Joe so that it looks like the message came from Alice.
• Bill includes the digital signature from the message Alice sent to him.
• Joe is convinced Alice sent the message!
Solution?

• Always start your messages with:
  - Dear Bill,

• Create a digest from the encrypted message and sign that digest.

• There are many other schemes as well.
Speed

- Secret key encryption/decryption algorithms are much faster than public key algorithms.

- Many times a combination is used:
  - use public key cryptography to share a secret key.
  - use the secret key to encrypt the bulk of the communication.
Secure Protocols

- There are a growing number of applications for secure protocols:
  - email
  - electronic commerce
  - electronic voting
  - homework submission
Secure Protocols

- Many application protocols include the use of cryptography as part of the application level protocol.
  - The cryptographic scheme employed is part of the protocol.
  - If stronger cryptographic tools become available we need to change the protocol.
Recall that validating a signature requires knowledge of the other party’s public key.

How do we know other people’s public keys?

Certification Authorities provide certificates that bind identities to public keys.

A certificate is a pair (id, key) signed by the CA.

A user needs to know only the public key of the CA.
Thanx ..... 

Any questions????????

Surabhi Singhal