

CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Introduction to Cryptography Tools

Symmetric vs Asymmetric Keys



Video Summary

- Advantages/Disadvantages
- Key Exchange
- Comparing the number of keys
- Comparing Generation
- Key Generation using Open SSL




Symmetric vs Asymmetric

Advantages/Disadvantages

□ Suppose 10 users need to communicate with each other

➤ How many symmetric keys need to be generated?


$$9 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1$$

45

➤ How many asymmetric keys need to be generated?

Each user just needs a Pair of keys

20

Symmetric vs Asymmetric

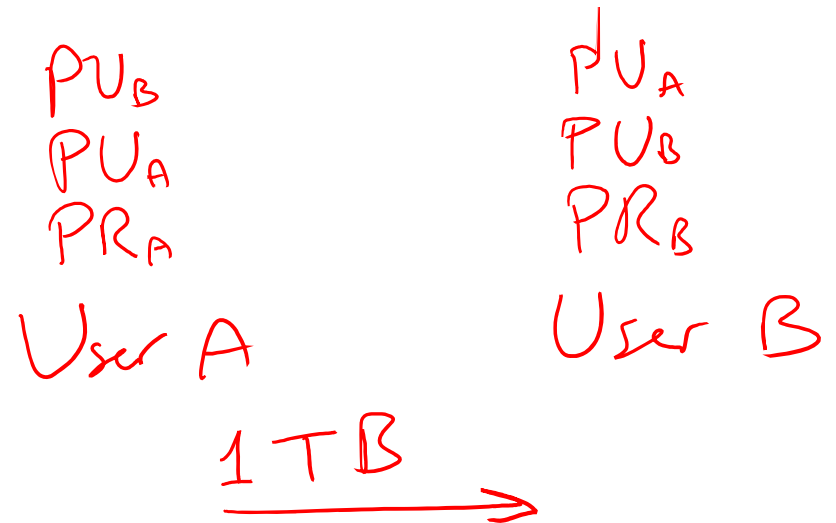
Advantages/Disadvantages

- ❑ Public key encryption is slower than symmetric key encryption due to the complexity of the algorithm
- ❑ Based on this, if you want to encrypt GB data then it is better/faster to use symmetric key encryption

Public Key Encryption Disadv
slow



Key Management/Exchange



- Public key: Trusted entity/organization
- Private Key:
 - ✓ Use the public-key encryption to securely send the symmetric key
 - This approach utilizes the advantages of both symmetric and asymmetric encryption mechanisms
 - Note that public key crypto algorithms typically much slower than symmetric key algorithms



Applications of Public Key Cryptosystems

Key exchange, share secret session keys

- Suppose we have two users (A,B) and A wants to send data to B using symmetric key encryption but still A wants to generate the symmetric key and send it to B securely.

A 1TB Data

B

Symm AES \Rightarrow K_{AB}

PU_B, PR_B, PU_A, K_{AB}

K_{AB}, PR_A, PU_A, PU_B

$C_1 = E_{RSA}(PU_B, K_{AB}) \longrightarrow K_{AB} = D_{RSA}(PR_B, C_1)$

$C_2 = E_{AES}(K_{AB}, Data) \longrightarrow Data = D_{AES}(K_{AB}, C_2)$

Keys Generation

- How a user can generate symmetric key?

1011001 → 1011001
A B

- How a user can generate an asymmetric key (private/public)?

Open SSL

<https://qsandbox.com/tools/private-public-keygen>

Keys Generation

<https://qsandbox.com/tools/private-public-keygen>

-----BEGIN RSA PRIVATE KEY-----

```
MIIEowIBAAKCAQEAAqk60EeuhImS2tUn/8MBrEEeqPZ8H1GhMKol3Fb55xNQrWAF/
31khZi5Sv2fJos0Kvz/atSoxpFf5M0wZKTmP+FiiglzqudR9fnFNqjklN+V36Nyl
tJyNI1gNnM8pJE4J0IT7rtEhMs/DHeTJfEq9f8u2qMEb0nrYh15ACA5i9mdj5Xcy
2sVLYtM0741ejTFvq8LrvvY/6xUOXOH2LjCjzBYAOk1q+GP5abZIVSn1VSYkd6GT
jdLQ7e3rUwn50c+Diu2oB2PNBrG5d0Qu3bxbA/cfEKxodp0Du+IRv6oknA0KrrN6
t9ea9t+nHUueJ93Rm+utWLGn0OotlwHRFWIz9wIDAQABAoIBAEE2VzTLcxWuFtjag
n5huEFg6TbQE3uxFF23JchbVz2N7xPKTVE1jrXN/ZvMLtTAVeO/nhxtBPZxA96YG
5O+C6bOZrW72JXjC9OjFdTw3DlZrXNUYr+S37RRM6Oam+Xcwlgb7kyVuSoMvDbC
l4gcBHhTtclRnmGM1VfV+BWzeCIH+ZmY+zUbgqmZql/AiPyjhfk7BOKd756qT/aE
BXkC6xP1rLJA+1+WPkBUfh7idIFqb9ANmy1cehqS2S6AOiA7bqJQb7NUul7Uhxjr
wMSgpDrdF6tHYIbWwFP4plln/lpeYSOg4VQy7uUPaV286p/OLAX/VVgYPLKq7NQ
q3MtngECgYEA0nd0yNAFNNFj+ZWwWgHA00yYM9t/aG/YZBBpz4ABqHsoTkbUrv2T
2OwWMG+7pZpYhg0rbX0DUes+Y/LI1ssbcPQf26Pe4N1vrax4HfWHLfze2/ss9QM
yQAvaYhdM7NpgTrhJ667pNpVnIFC3BUqJuS7CSpwkfsUDdule9NF9V8CgYEAzycP
lcleRbfhOECpW9B6yR2UpYZsiHvzclMjvi+cwaQZhx1t1Nie9VlmkhUVfI5Oiz
PW5yaolpvAuwsxBhp36vQClkRJYN+Cre6dVJfvKP9vgC1BE2/kbe4b5y9FF/ODE2
1+5R/RC2xLIVKg1TmvHD3sjAe3efiNaOSA4JcGkCgYACikyPi+s0Kv7Q6VylFpBS
ZudDYPfVs9vhwUz1oy7h8LKY10QD5K2fJaJS7VZPdmBxJcGLbcHXgEZdgHYBij0s
Cfv/Pb9f10OZjKzy759W82Vt7PjnZrzMxELOPEYbtKOMWqaTCwnawIPeArVi4KKE
m6giQS/goy4nyKnjp7YlcwKBgQCvWE6Usq3RMc6wQOXwSB5G8oUKf3iLJ8W9qKkD
NEZxMxMzeNXsnDKwGSiHQsHzCq2AJgDidQTgZwFQrUyKpckjcDaDxwWakLGOaSt7
HxExJbz6vgAW5eN45SBwUTcY24smWPKqYI6B+Y3bfSoxCERgkVLLN37GhAFEYOja
ORboUQKBgGDW/LqKln+npfdbg+0y4bHChPnYnAdGnwNU9072kba5gCXgrQ5iBI52f
J+VRhoKwuir3H05l6CHYf26sDltzZbdSvubHUMNdr1Xu9PMins9bahl307x+3WVv
eOAW+IJKF1fUXIwTGuJtjSMRfTlVPvwpCW5nENL2sV3NREqN9Oc
```

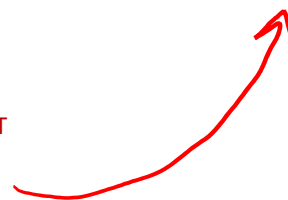
-----END RSA PRIVATE KEY-----

<https://qsandbox.com/tools/private-public-keygen>

-----BEGIN RSA PRIVATE KEY-----

```
AAAAB3NzaC1yc2EAAAADAQABAAQACqTrQR66EiZLa1Sf/wwGsQR6o9nwfuAewqiXc
VvnnE1CvAAX/fWSFmLIK/Z8mizQq/P9q1KjGkV/kzTBkpOY/4WKKCXOq51H1+cU2qOSWf
5Xfo3KW0nI0jWA2czykkTgnSVPuu0SEyz8Md5MI8Sr1/y7aowRvSetiHXkAIDmL2Z2PldzLa
xUti0zTvJV6NMW+rwuu+9j/rFQ7E4fYuMKPMFgA6TWr4Y/lptmVVkfVVLlp3oZON0tDt7e
tTCfnRz4OK7agHY80Gsbl3RC7dvFtr9x8QrGh2nQO74hG/qiScDQqus3q315r236cdS54n3
dGb661YsafQ6i2XAdEVYjP3
```

-----END RSA PRIVATE KEY-----



Open SSL

Cygrwin

➤ OpenSSL is a program and library that supports many different cryptographic operations, including:

✓ Symmetric key encryption ✓

✓ Public/private key pair generation ✓

✓ Public key encryption ✓

✓ Hash functions

✓ Certificate creation

✓ Digital signatures

✓ Random number generation

Video Summary

- Advantages/Disadvantages
- Key Exchange
- Comparing the number of keys
- Comparing Generation
- Key Generation using Open SSL

