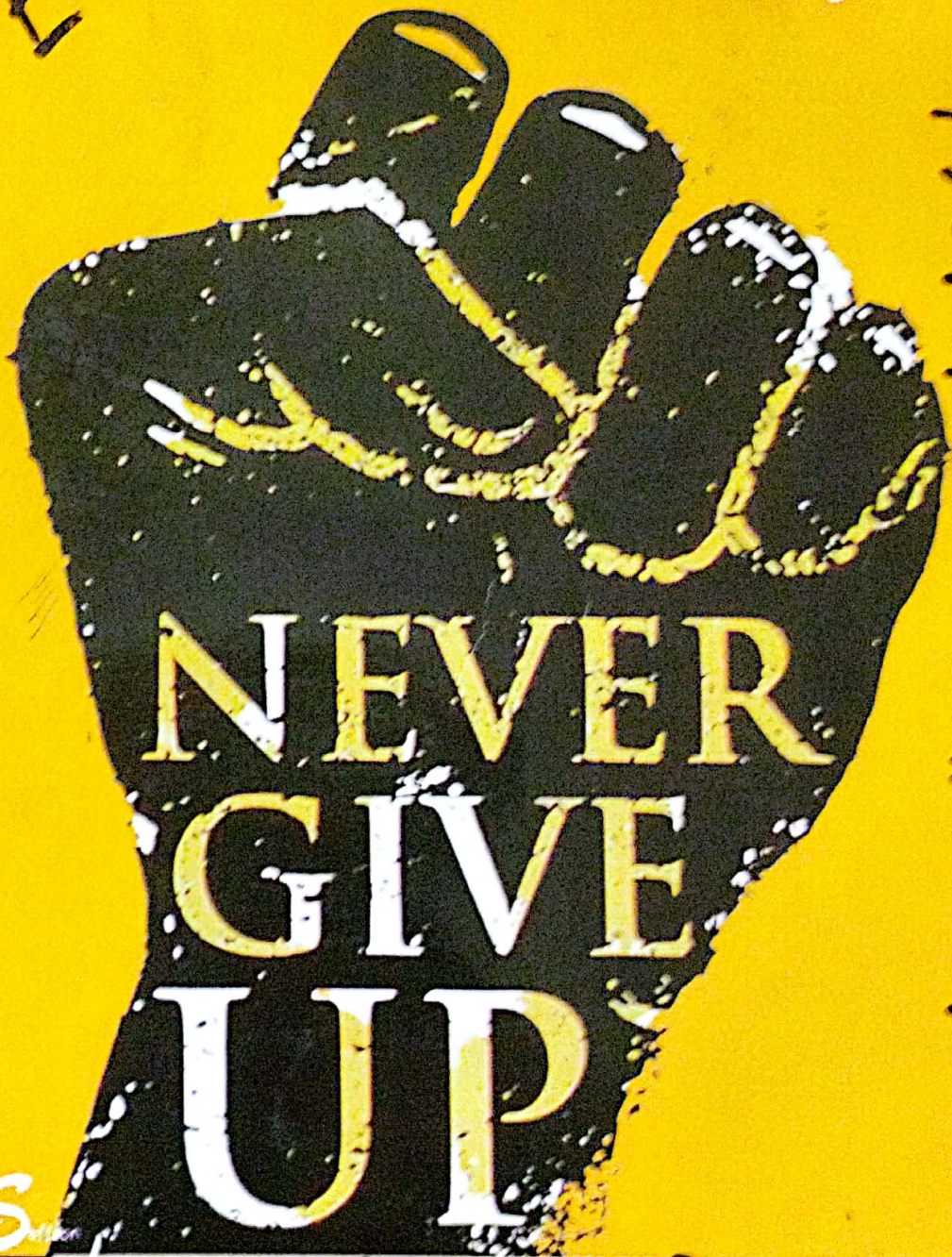
CSE487 (RDA)

2020-1-60-215

INSPIRE



Cyber security, Ethics and law

Name Md. Abdul Ahad Rifat

School/College

Class Section Roll No Shift

Subject CSE487 Year

2023

OSI = Open System Interconnecti

ICMP = Internet control Message Protocol

IP = Internet Protocol

UDP = User Datagram Protocol

TCP = Transmission control protocol

ARP = Address Resolution Protocol.

MAC = Media Access control.

LAN = local / Area Network

W — World

P — Personal

M — Metropolitan

Oct 2023 CSE 487 (section – 3)

class test

2nd project → case study + viva
(individual viva)

3 project → 15 + 15 + 15

main topic → cyber security

Xubuntu/Bodhi / kali / fedora.

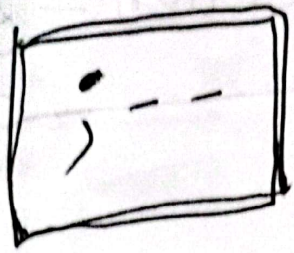
course out core → 3 1 credit course.

local and Global - law —

Book → williams

understand
cryptography

TryHackMe → Linux Fundamental complete
beginner.



→ SQL injection

Security Auditing
↓
Penetration Testing

Security vulnerability Hacking.

Red Team	Blue Team	Purple
Attack	Defend	Help Blue Team to fix the issues

Port swigger

SQL injection

RED TEAM

ATTACKERS

Works to break into the system.
Skills include:

- Penetration Testing
- Vulnerability Scanning
- Social Engineering
- Threat Intelligence
- Custom Toolset Development

PURPLE TEAM

MEMBERS FROM BOTH TEAMS

Gets blue and red teams to work together to improve an organisation's security posture.
Skills include:

- Collaboration
- Information-Sharing
- Reporting and Analysis

BLUE TEAM

DEFENDERS

Works to keep the systems safe.
Skills include:

- Network Monitoring
- Data and Log Analysis
- Risk Assessments
- Threat Detection

Debate

Poster

Cyber security Fundamental

Network security Essentials

Chapter - 1

CIA →

encryption

Hide something

Hide the msg.

confidentiality

steganography

so hide the communication among the audience.

Diffi Hellman Algorithm

magic ink

Digital Steganography

Dual

~~Integrity~~ base means এত প্রকারের variation

Hack

WSY

0
1
base-2

0
1
2
3
4
5
6
7
base-8
2^3

0
1
2
3
.
.
8
9
A
B
C
D
E
F
Base 16 = 2^4

base64

$2^6 = 64$

বাইনারী data 6 টা 6 টা করে গ্রুপ করে

crypti...

Cryptii

Binary — Byte.

encoding

base64 table

translate for -

Base 64

Racecar

Question.

ASCII

to binary to base 64 →

8 bit binary.

Encryption

EWU → Plainte

+2

Ciphertext ← GYW

EWU (-2)

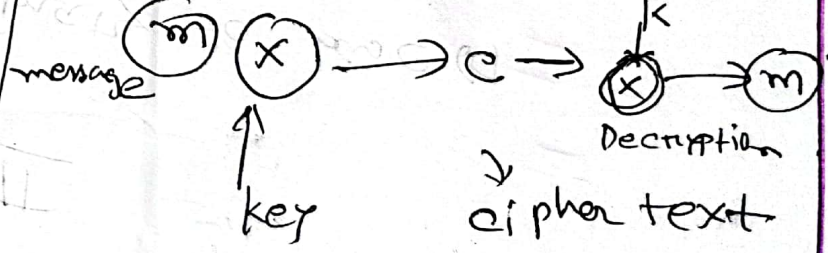
decryption.

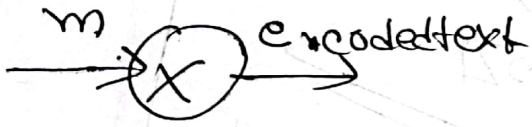
Encoding one kind of Translation.

Encoding

key we all need

Encryption





key depend on encryption so encoding do not need key.

Wikipedia
https://en.wikipedia.org › Kerckhoffs's_principle

Kerckhoffs's principle

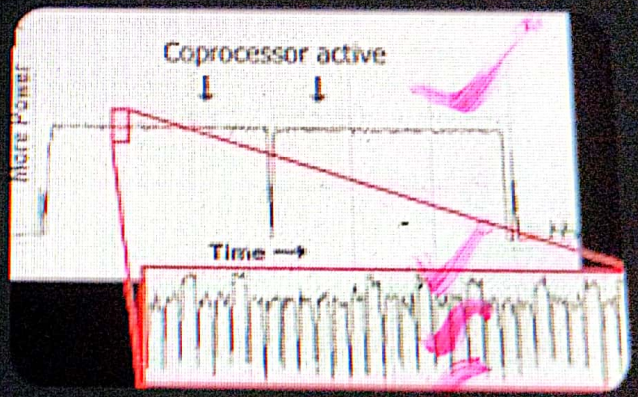
The principle holds that **a cryptosystem should be secure, even if everything about the system, except the key, is** public knowledge. This concept is widely ...

Missing: ~~k khofs~~

People also ask

What is Kerckhoffs's principle explain?

In the late 19th century, Dutch cryptographer Auguste Kerckhoff postulated what has become known as "Kerckhoff's Principle" — **a cryptosystem should be secure even if everything about the system, except the key, is public knowledge**. Since Kerckhoff's days, cryptography has certainly evolved. Sep 21, 2020



rambus.com

Theme: Class-2

Date: 9 / 10 / 2023

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

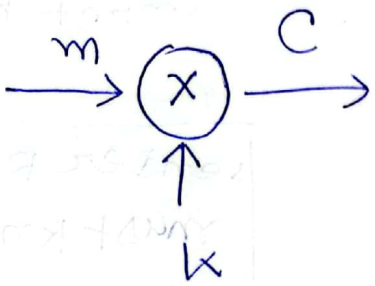
Kerckhoffs Principle

m = message/plaintext/cleartext

k = key

c = cipher text

Sender



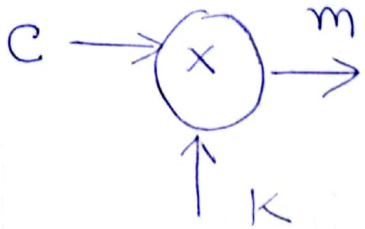
encryption

$e(m, k) = C$

$d(C, k) = m$

decryption

Receiver



cipher = encryption Algorithm

---

m = "Hi" → Hi message 2 step further

k = 2

$e(m, k) = C$ = "Jk"

So this encryption (m + k)

(H) 8 + 2 = 10 (J)

(i) 9 + = 11 (k)

Encryption Algorithm must be free (Public) or open

Theme: Caesar Cipher Date: / / ☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

decryption → $d(c,k) = m$

$(c-k) = 10-2 = 8\ (H)$

$= 9\ (i)$

Brute force

All combination Apply

ATM → 4 digit

So break $10^4 = 10,000$

(0 to 9)

Algorithm open but value means key not open

$k = ?$

secret key

sender Receiver must know the key

Core i 7
1 min
4.5k password break

4500

Attack surface low → only three times allowed.

Theme:

Caesar cipher → Cryptii

Date: / /

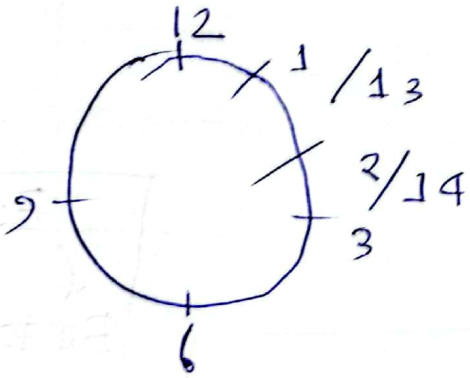
Sat Sun Mon Tue wed Thu Fri

secrecy of the secret key — Kerckhoffs's principle

Modular

$14 \% 12 = 2$

$28 \% 26 = 2$



MetaData →

Attack (Traffic Analysis)

Security Engineer

- Brute Force
- Traffic Analysis

Signal code → open for everyone to verify.

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Wireshark

evas dropping → ডাটা ক্যাপচার

Software

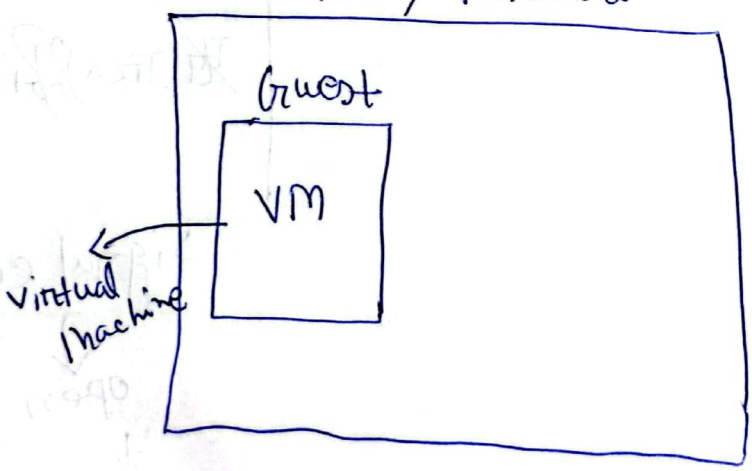
network Miner

E2EE

End to End Encryption

virtual Machine

Host = physical Machine



Snapshot

vmware

Theme:

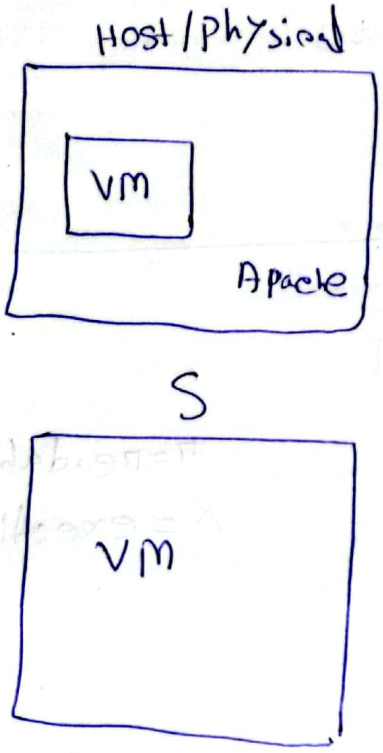
Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Server

↓ ↘

physical virtual

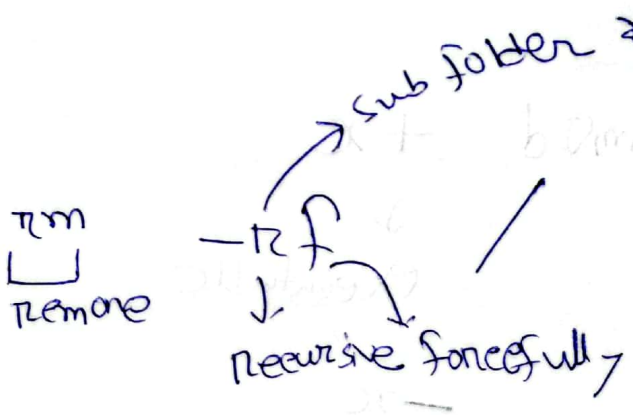


Apache2 → Web

bind 9 → DNS

MySQL → Database server.

Delete করব~



/ → root folder

Linux is case sensetive

---

linux file → owner

④ ② ① → other.

group r w x

r = readable

x = executable

Chmod

---

install.sh

↓

Shell script

chmod +x

↓

executable

-x

↓

remove executable.

Theme:

Date: / /
□Sat □Sun □Mon □Tue □wed □Thu □Fri

windows

Cd
↓
change directory

cd .

chmod +x .
↓
current folder.

..
↓
parent folder

chmod +x ./install.sh
↓
current folder ⇒ under ⇒
install.sh

> ./install.sh

---

sudo rm -rf /
↓
sudo means administrator

Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Theme:

Confidentiality

Steganography

বুঝতে দিচ্ছি না কখন তথ্য কথা বার্তা বলতেছে আর কখন বলছে না।

Traffic Padding

Attacker pattern খুঁজতে পারে না

Security mechanisms

Encryption same as Encipherment.

Integrity

Alice —— Bob

"Hi" "bye"

X

Gwrantte mathematically

Hash

Theme:

Date: / /
□Sat □Sun □Mon □Tue □wed □Thu □Fri

SHA-1 → 160 bit

SHA256 → 256 bit

Well known

SHA-384

SHA-512

7-Zip

CRC SHA

hash is a function

h(m) = digest / hash value / Sum / Checksum

m → message

h could be

SHA-1,

MD5

SHA 256

Linux

Sha256Sum(filename ka)

3.9G

= [256 bit value]

256 bit value.

3.9G

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Input যত বিট হোক output 256 bit.

SHA256 Sum

Sum =

7-Zip

SHA value check with website value

If same then Integrity ঠিক আছে।

kali linux sum value

Theme:

Date: / / ওয়েলকাম

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

William stallings → Network Security essentials

3.2 page 67

1 bit 3 যদি change হয় Hash change হয়ে যায়।

Internet হলে Cyber

Digital হলে cyber হত 3 থাকে না 3 থাকে।

File কে corrupted করে কিনা, Temper করে।

File অপরিবর্তিত নাকি না Hash দেখে বুঝবেন

Digital copy

Forenecics Investigation

using Device

যদি data delete মুছে গিয়ে

Chain of custody tracking form

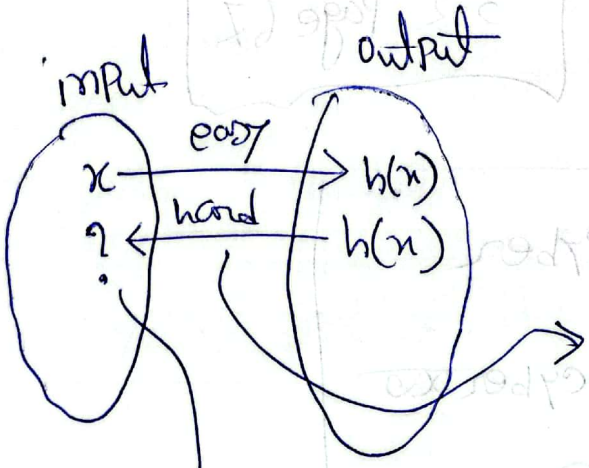
Digital ও chain of custody / Integrity Ensure করে।

Hash backtrack Never Possible.

Date: / /
□Sat □Sun □Mon □Tue □wed □Thu □Fri

Theme:

Hash is one way function ⟶



কে x এর value টা বের করে দিতে পারবে তার bitcoin পাবে

Avalanche
↓ (তুষার ধস)
সামান্য change করলে
output drastic huge
change হবে,

3.2 Secure Hash Functions

Rainbow Table

Name:

Date: / /

gpu performance better

Rainbow 🌈 Table

gpu performance better in particular operation
because of parallel processing and number of processor

Theme:

Date: / /

□Sat □Sun □Mon □Tue □Wed □Thu □Fri

Not secure
↓
to secure

Wireshark
↓

Cryptographic Hash

Hash to is one to one and one way function

input জানলে

$$x \xrightarrow{\text{easy}} h(x)$$

$$? \longleftarrow h(?)$$

↓

very hard

↓

করা গেলে বুঝা যাবে Hash function ভাঙা

Hash যেকোন size input নিতে পারে but output fixed

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Suppose SHA-256

3.5Gb, 1Kb ⟶ 256 bit

passport. gov. bd

Hash is one way function

h(x) → Digest / checksum / sum / image

(Pre image) x ⟶ h(x)

easy

one way and pre-image same

brute force → try all possible combination

bit coin mining

Hash Reverse.

bit credential

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Rainbow table

↓

known Table where we can see the hash

Avalounge effect

↓

ছোট্ট change এর ফলে বড় ধরনের change.

Rainbow Table effect minimize using Random salt.

Theme:

digital

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

File is more Harmful.

Hash chain

Hash match করব

Forensics sale

FTK@ Forensic Toolkit

Feature Color

Encase

autopsy

kali built in

undelete

যাহা ইচ্ছা তাহা delete করে দিব

Fixed Length output.

1) H can be applied to a block to data of any size

2. H produces a fixed-length output.

page

willan stallings

Theme:

Date: / /

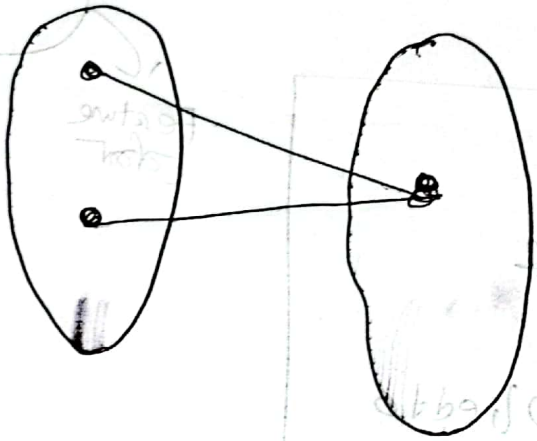
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

$x \longrightarrow h(x)$

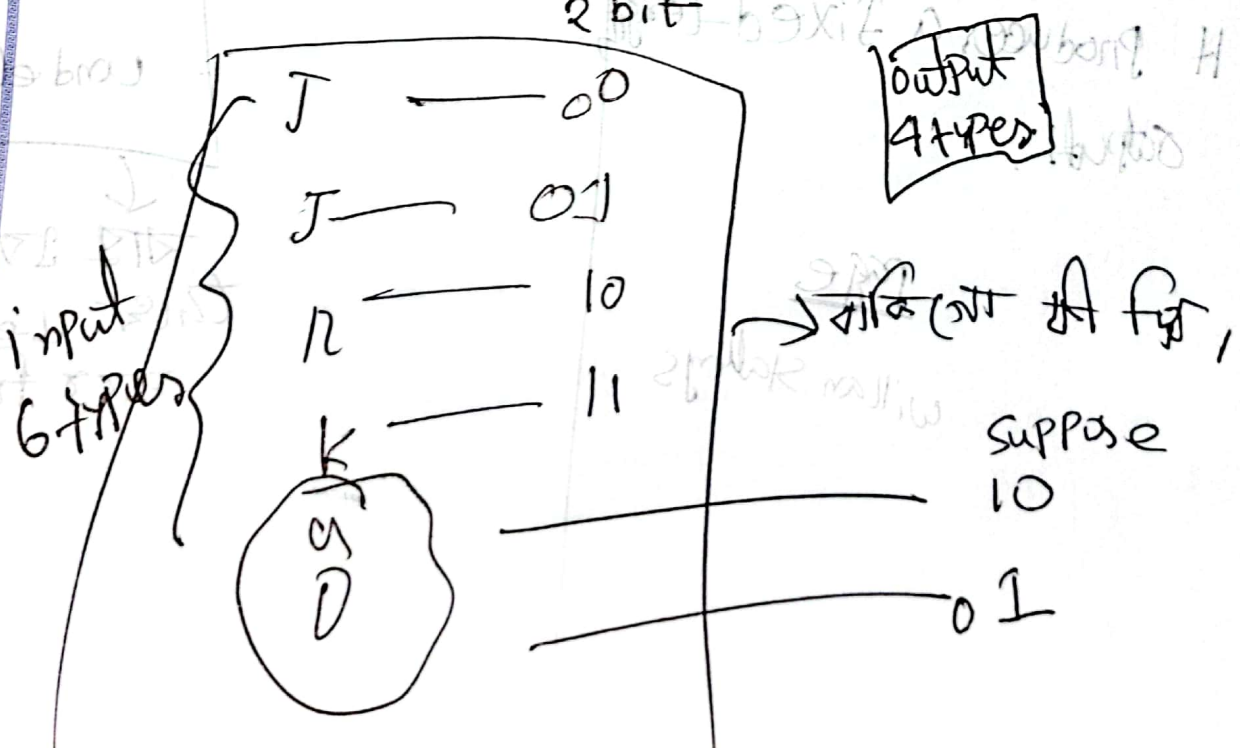
$\neq$

$y \longrightarrow h(y)$

hash collion হওয়ার সম্ভাবনা



Suppose 2 bit ফ্ল্যাশ



Theme: Here collision occur.

Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

input variation endless.

machine learning → Statistics → pattern Recognition

Hash collision খাওয়ার অনেক easy

→ birthday paradox

→ same birthday posibility

Number of collision dramatically low..

75 জন হলে 90% Change

23জন 50% Chance

2জন এর মধ্যে মিল পাব

Theme: Date: / /
□Sat □Sun □Mon □Tue □Wed □Thu □Fri

The Math behind birthday paradox.

$$1 - \left(\frac{364}{365}\right)\left(\frac{363}{365}\right)\cdots\left(\frac{365-n+1}{365}\right)$$

$$1 - \frac{365!}{(365-n)}$$

Virtual Machine Snap

Linux File Sharing without 'internet

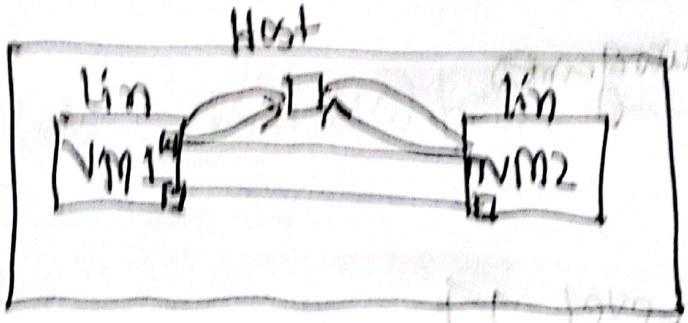
Virtual Machine clone

All kinds of.

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐Wed ☐Thu ☐Fri



Remote Folder load.

↓

mount command

wiget/curl

File download sep

wget

lsblk

↓

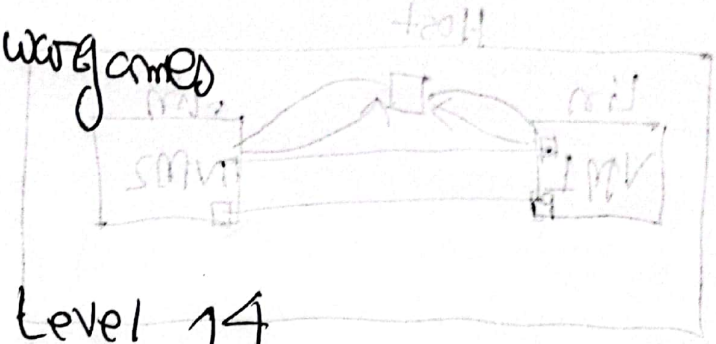
partition দেখার হলে ব্যবহার হয়।

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

bandit wargames



↓

pass level 14

ssh

↓

secure

shell

↓

teamviewer

Theme:

SSH default port 22

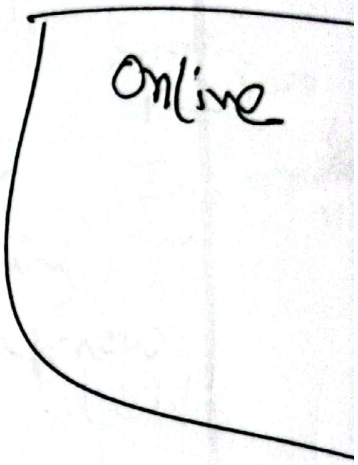
Date:

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

ssh bandit0@bandit.labs.overthewire.org -p 2220

termux for phone

file sharing



cat ./New Text Document.txt

dir

↓

directory

Bandit walkthroughs

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

•

↓

dot from hidden রয়েছে,

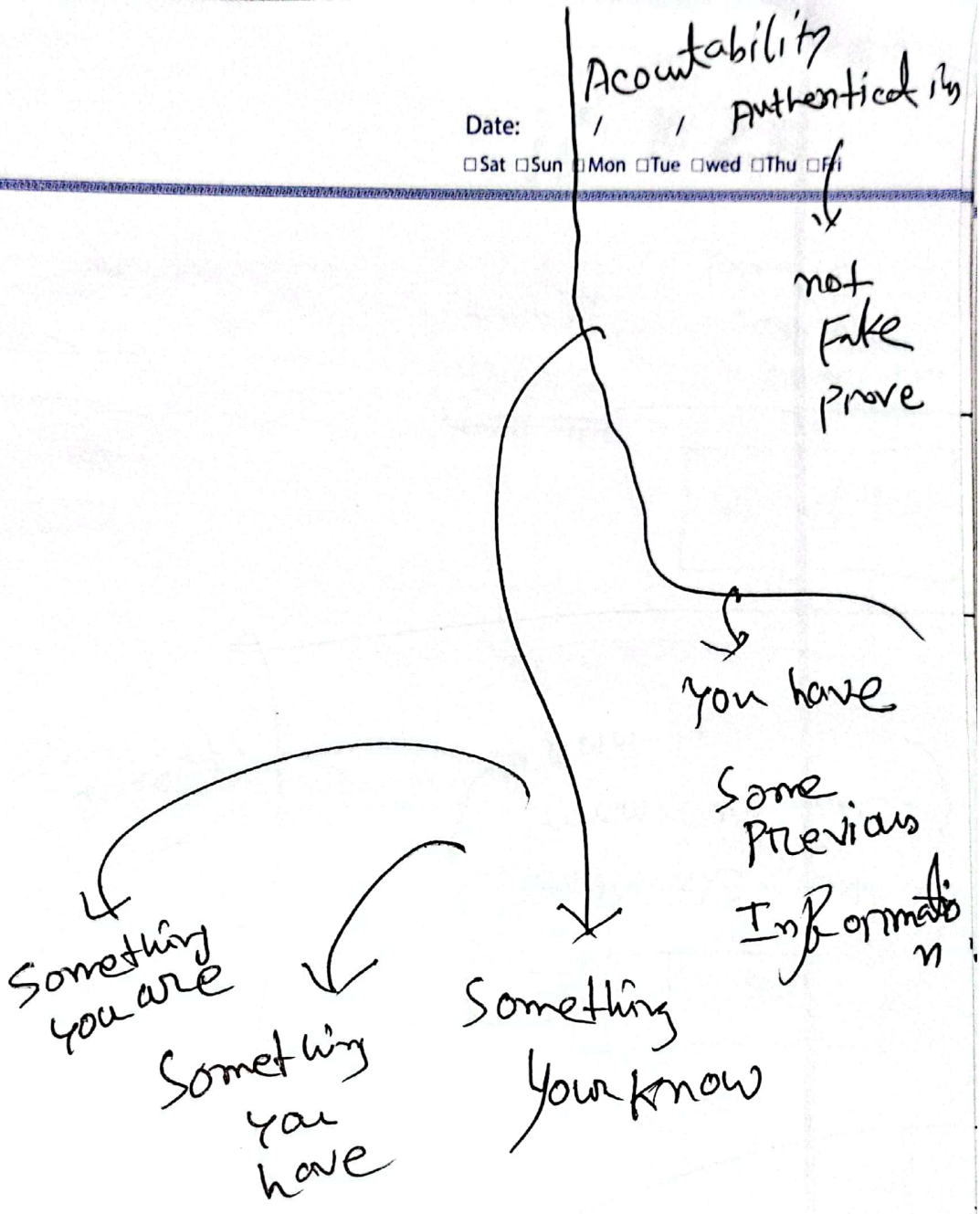
Type

↓

File এর Type

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri



middle

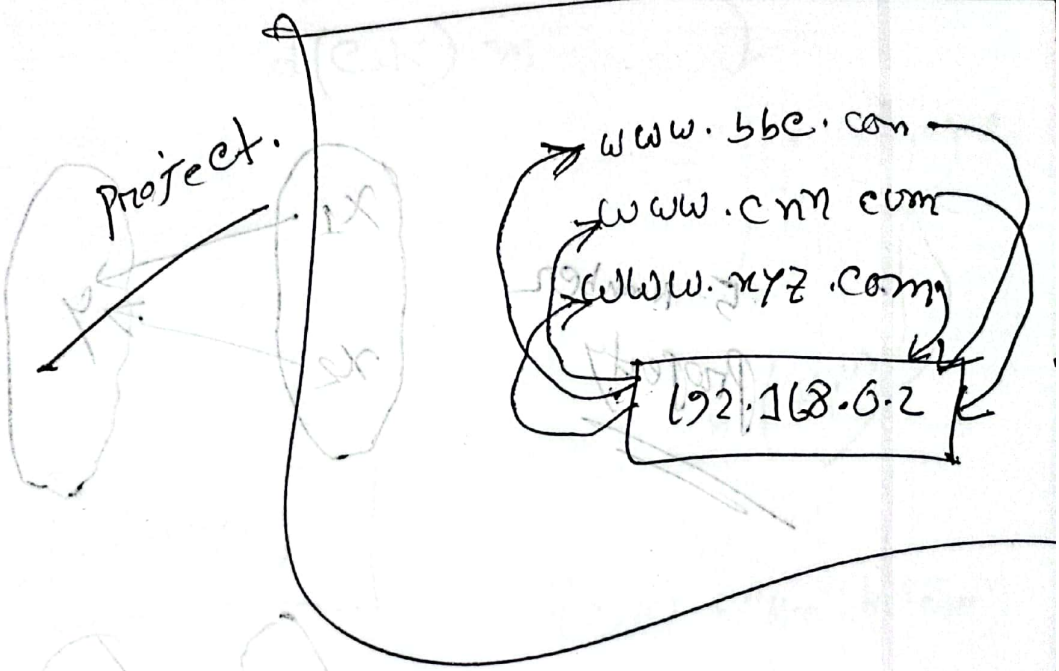
Date: 16 / 10 / 23

□Sat □Sun □Mon □Tue □Wed □Thu □Fri

Remote Desktop connecting

Virtual Host

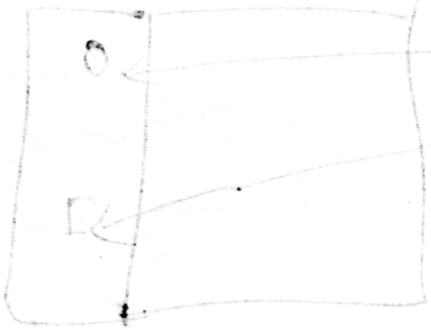
wiki.



nslookup

↓

name server look up.



Theme:

Date: / /

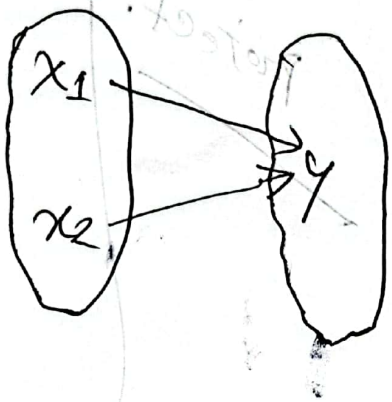
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

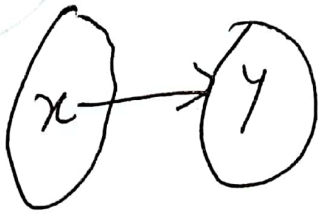
☒ Hard to reverse

☒ Hash collision

second preimage resistant

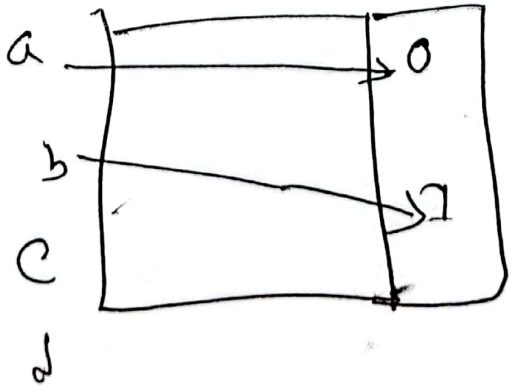
5 Number Property





$x \rightarrow h(x)$

$y \rightarrow h(y)$



Theme:

m = "Hi"
$m = m \,||\, h(m)$

□Sat □Sun □Mon □Tue □Wed □Thu □Fri

m = "Hi" $h(m)$

m' = "Hi, h("Hi")"

$e(m,k) = c$ —clear→ $d(c,k) = m$

$d(c,k)$ m

= "Hi, h("Hi")"

h("Hi")

m = "Bye", h("Hi")

$d(c,k) = m$"Bye", h("Bye")

h("Bye")

Man in the middle Attack

Sophisticated

Bird suite

we Proxy in Antartica and canada.

Availability

Service

Wifi hacking

Router অথবা তার access Point.

Networking

Jamming

pencil battery Hack

Mocker Hunter

Disociation

4way Handshake

Reason

broadcast

Router

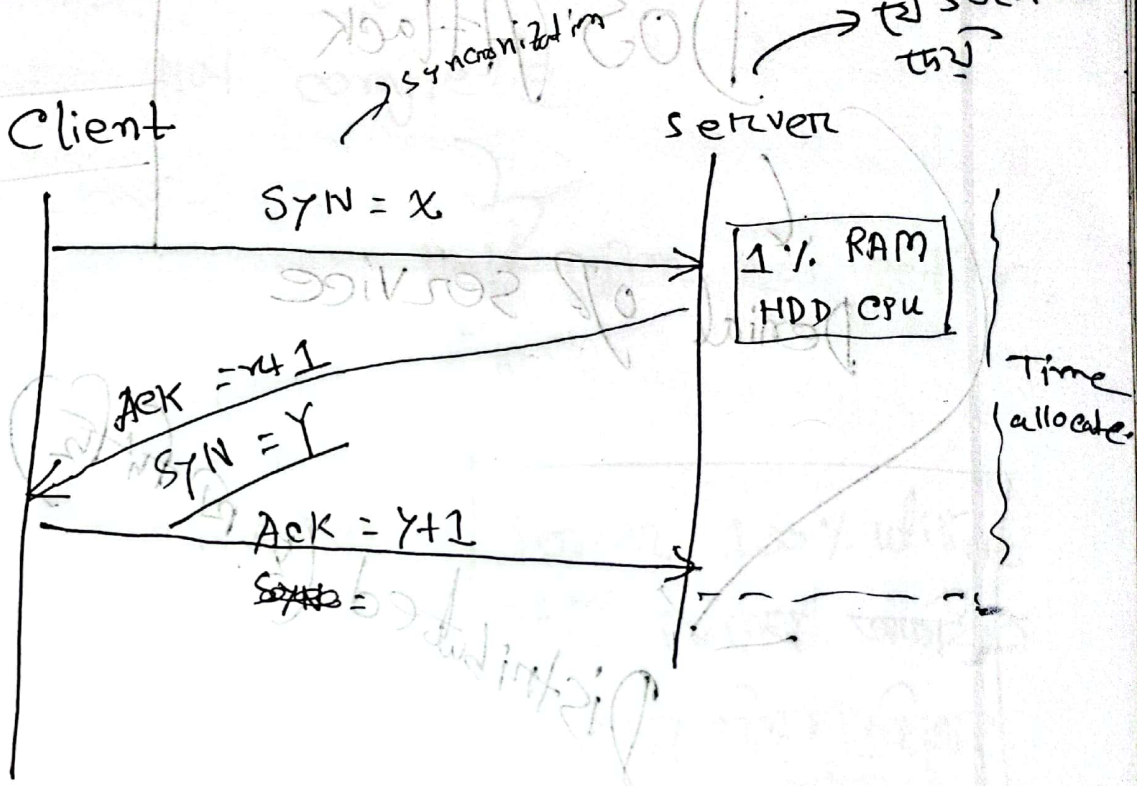
10,000 Packet send.

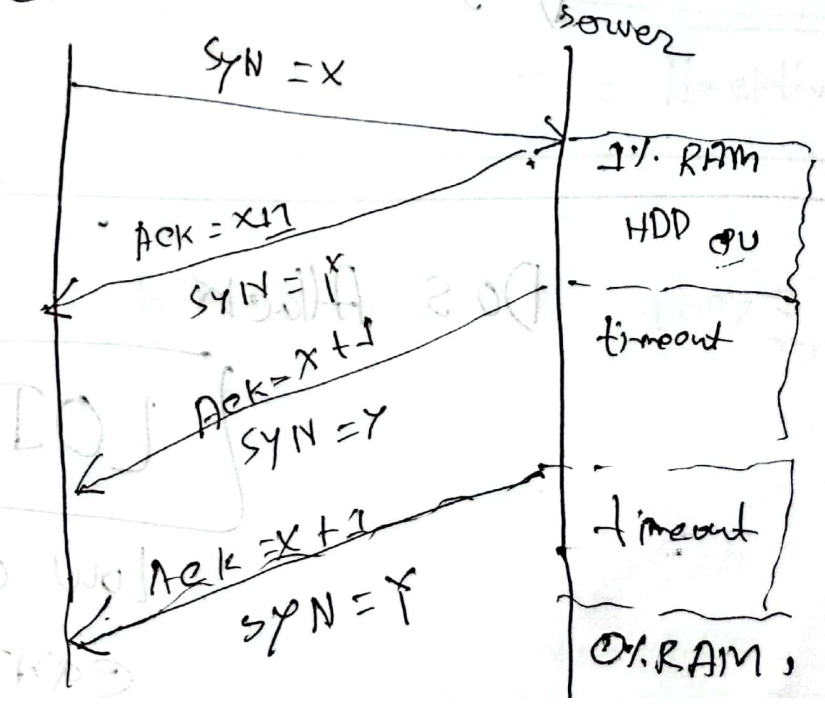
Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

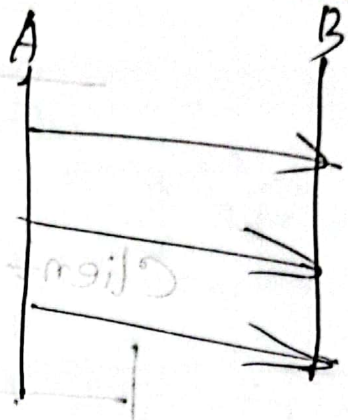
3 way Handshaking





Theme:

100 Request



100 বার অতিরিক্ত রিকুয়েস্ট পাঠায়। Server কে crash করে, আক্রমণ করে দিয়ে ইন্টারনেট

DOS Attack

Denial of service

Distributed (ছড়িয়ে ছিটিয়ে)

DDOS

Dos Attack

LOIC

Low orbit Ion cannon.

Theme:

Banglider there 100 Hat Dure

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

3 way Handshaking

Not complete

Half open connection.

seenflood Attack

Server 100% utilize করে যেন অন্যরা ব্যবহার করতে না পারে।

Hacking + Activism = Hacktivism

tortan horse

troy ? movie.

Social Engineering

Non technical Hacking.

Theme:

Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Zombie PC

Ready

attack

botnet

attack

(Deep web)

Dark web search engine

ash mia

ash madia.

utilization

outgoing

Theme: on bot father

Date: packet in packet

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☑Thu ☐Fri

Firewall based on some rule.

~~botnet~~ Father is a server where server pc are connected means Zombie pc. So, this pc use to possible the DDOS attack

bypass

---

botnet [illegible] তৈরি কর [illegible] তারা steganography use করে, byte-Array

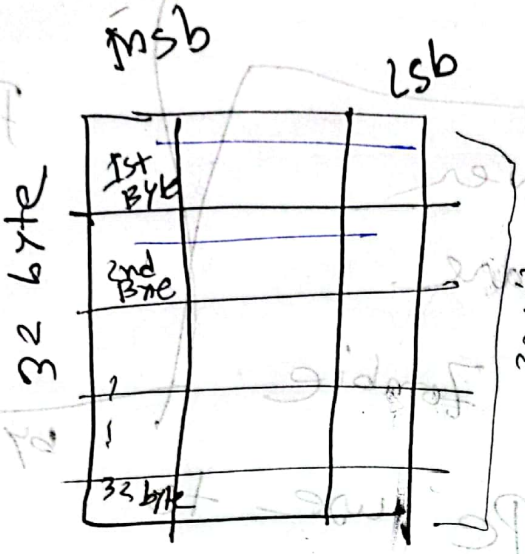
32 bit

ip address

steganography.

Theme:

Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

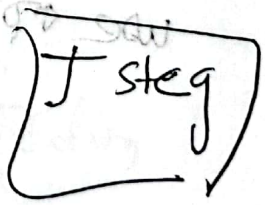


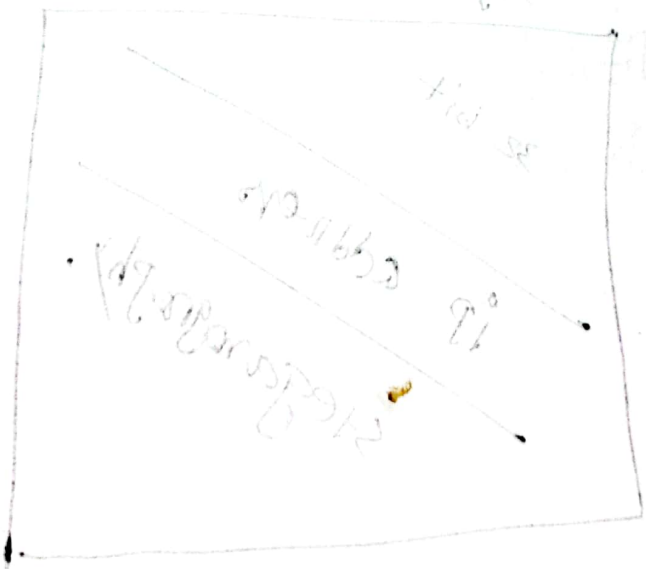
103.192.3.4

32 bit

suppose 1st 32 byte এর lsb এর value হচ্ছে 1st

LSB Steganography.





Theme:

Date: 18/10/23

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Captcha

Completely Automated Public Turing test to tell Computers and Humans Apart

2^7

$2^8 = 256$

$2 = 512$

#ffffff

4bit = 24 bit

24 bit color

digital watermarking

captcha we for stop Automation

we stop botnet using captcha

Recaptcha (check mouse movement)

DNS Provider (cloud flare)

1.1.1.1

Provide Recaptcha and captcha

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Confidentiality + Integrity + Availability

system security Active

Accountability → দায়ভার (এড়িয়ে যাওয়ার সুযোগ নেই)

(Non Repudiation)

Single

Something your are

Something you know

Something you have

distributed

multifactor (2 factor authentication)

Authenticity

sim card, ATM card } 64 KB

hash of that share secret

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Something you know → distributed

slide

NIST

Cyber Security Framework Provider.

RFC 1035 DNS

RFC 793 TCP

RFC

Request for comment for standardization

Standardization is needed

SIG2. Specialist Interest Group.

Theme: Network Security Essential

Date:
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

OSI

Open System Interconnection

RFC 2828

Glossary

2

Dictionary

RFC 4949.

Application Identify

↓

~~using~~ Port number.

every communicating we use address

Theme:

Date:

Obsoletes = বন্ধ
চেহারা

THE OSI Security Architecture

↓

সবাচেয়ে
আগের
Random
লোকসমূহ
same
Channel
Follow
করে Communication করে

X.800
↓
Security Architecture.

$X_{86} \rightarrow 32$ bit

$X_{64} \rightarrow 64$ bit

Threats and Attacks → যদি হয়

হওয়ার chance
আছে কিন্তু
হয় নি
vulnerability

chance
আছে → যেই জিনিসগুলো বাড়ান
হইছে

বেশি ক্ষতিকর হইলে।

Levels of Impact of Security breach

Theme: Date: / /
□Sat □Sun □Mon □Tue □wed □Thu □Fri

CVE → search google.

↓

Common vulnerabilities and exposures.

NVD → National vulnerabilities Database

---

exploit →

↓

weapon

→ malicious piece of code

↓

verb → code that executes

0 Day vulnerability

↓

recent ~~detected~~ invented.

VPN

Exploit db

dark web

Exploit use করা হয়

Obfusecation

wikipedia

Libary

code obfusaction Libary use করে file তখন antivirus ডি[illegible] না। [illegible]

Theme:

Date: / /
□Sat □Sun □Mon □Tue □wed □Thu □Fri

common vulnerability Exposure.

Enumeration -

CVE then

Exploit then

Social Engineering.

Alt 0 1 0J

↓

un Transparent file.

- use permission manager
- use latest Technology.
-

Google Hacking Database

google dork

intitle:index.of back or the puter html

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu

google dork redmicte database

Threat

↓

system warnyair

CVE and NVD

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

if 256 bit

so,

0 and 1 binary represent

$2^{256} = ?$

total 8 bit

and we denote in Binary number where binary represent 0 and 1

means 2 number

so,

2^n = here number is 8.

so, $2^8 = 256$

if we use 8 bit number in decimal

so,

0, 1, 2, 3, 4, 5, 6, 7, 8, 9

(10)

$10^8 = ?$

0, 1, 2, 3, 4, 5, 6, 7

8

8bit so

$8^8 = ?$

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15

A B C D E F

16

$16^8 = ?$

Theme:

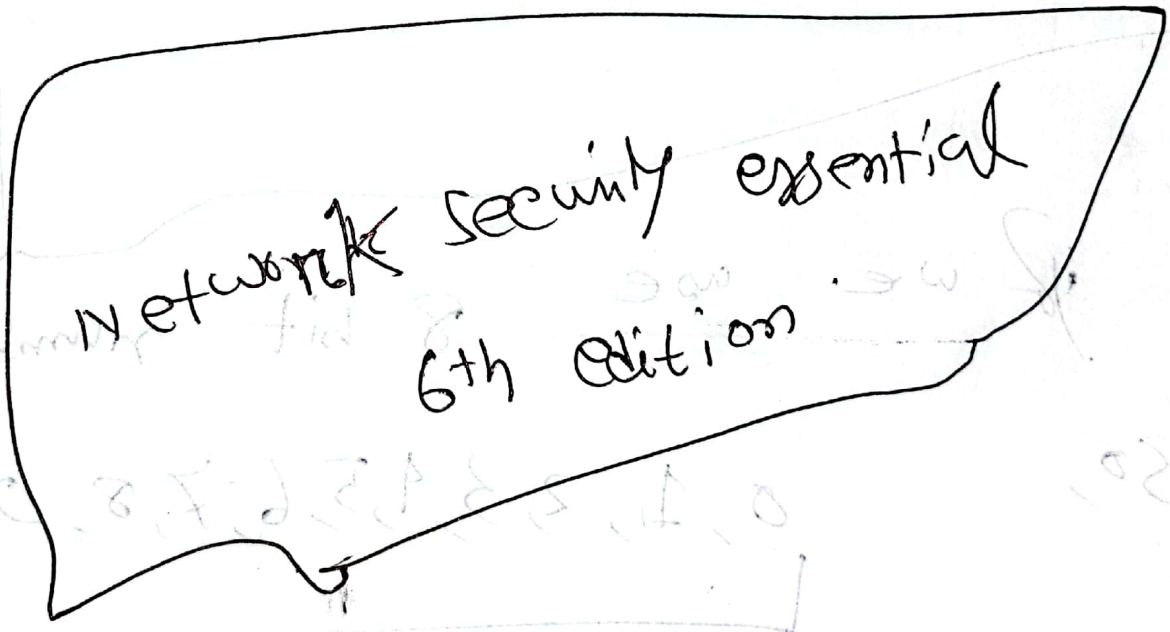
☐Sat ☐Sun ☐Mon ☐Tue ☐wed

Firewall

Security Attack

security mechanism → noun

Security service

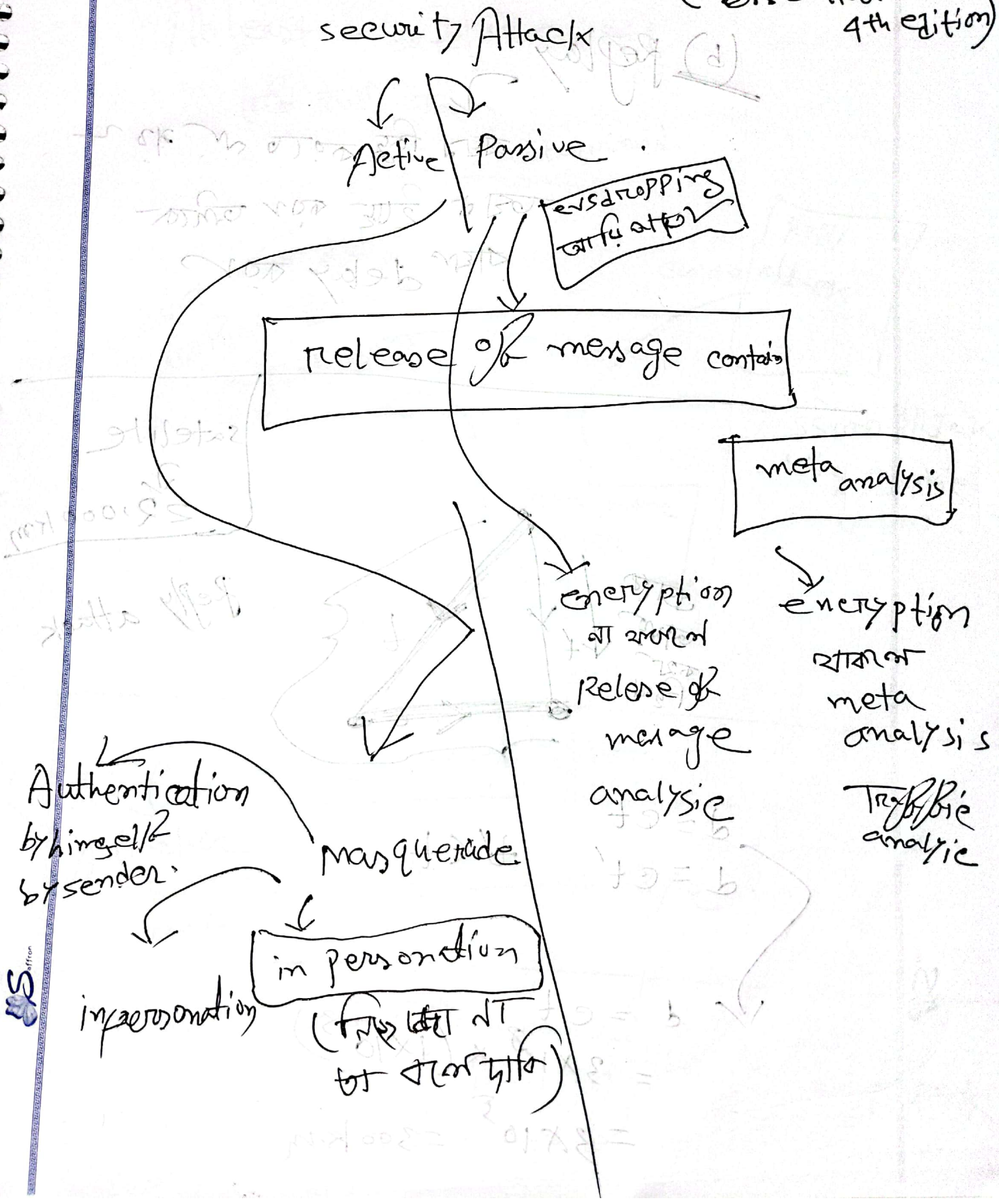


Theme:

Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

stalling williams (Network security essential 4th edition)



Theme:

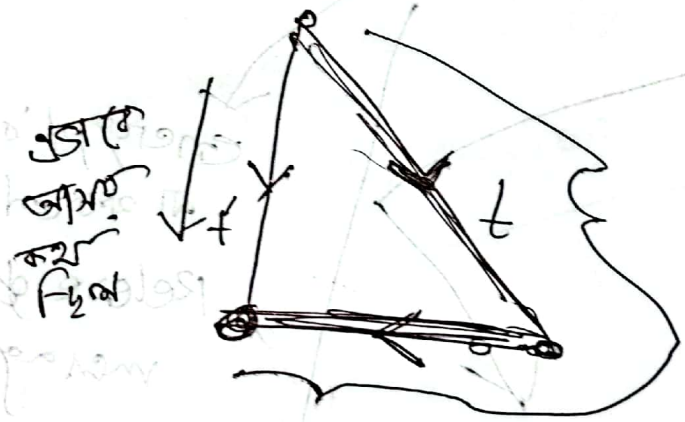
Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

(b) Replay

যখন কিছু করতে না পারে তখন ইচ্ছে করে অন্যকে বাধা delay করে

satelite
↓
22,000 km



Reply attack

$d = ct$

$d = ct' \quad t' < t$

$d = ct'$

$= 3 \times 10^8 \times (1 \times 10^{-3})$

$= 3 \times 10^5 = 300 \text{ km}$

Theme:

→ nothing change

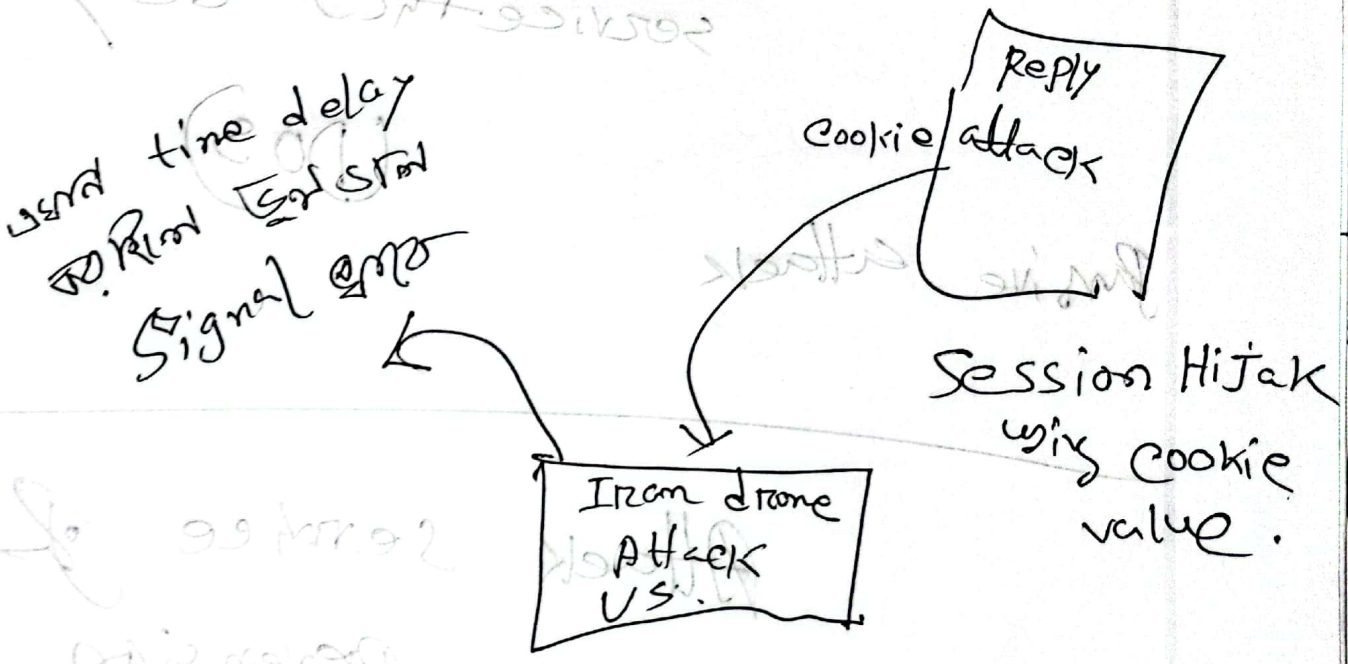
Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

At least 4 satelite needed.

কেন হলে তাদের ?

overditermined.



(C) modification Attack

Attacker change করছে

Hi ⟶ Bye.

MITM ⇒ Man in the Middle Attack

Theme: Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

(d) Denial of service → function not
{
service not deny.

(DOS)

Passive attack

Attack service prevension.

Release of message content

Table 1.3 (security Mechanism)

Table 1.2 Security services

William Stallings
↓
Network Security Essential 4th edition

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu

traffic padding

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Cryptograph and Network security

7th edition

chapter 1

1. Attack surface and

Net work security and essential

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

DOS

Ratelimit

Cloudflare

What is server bandwith

Release of content.

4th edition

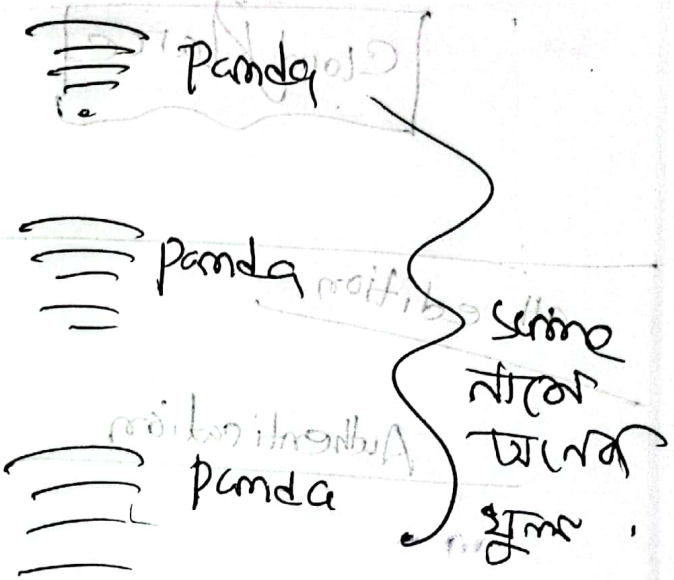
Authentication	Data Integrity

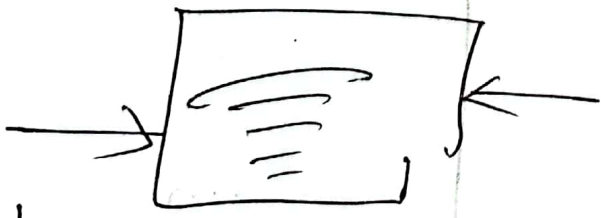
Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Deauthentication





Bombado attack.

2.4GHz ৬ Range বেশি Speed কম

5GHz ৫, Range কম Speed বেশি.

Theme:

Date:
□Sat □Sun □Mon □Tue □wed □Thu □Fri

Access control

New user create if any services so if one service hack or compromised other will be not.

Different service Different user.

Apache HTTPserver	DNS server bind
↓	↓
one user name and its admin.	one user name and its admin.

↓

no root user choose because if get then whole system is compromised.

Theme: RSCDA Date: / / Sat Sun Mon Tue Wed Thu Fri

PCL 2

Access control

No repudiation

↓

Accountability

↓

পরিচয় প্রমাণের না, পরিচয় কে পরিচয় প্রমাণে বাধ্য না তাই কে

Theme: Date: / /

buffer overflow

যেটার extra জায়গা থেকে malicious piece code দিয়ে কোড়ে যাতে সেই memory address হয়,

---

Cross site scripiting

html heder এর ভেতরে scripiting code malicious, browser বসিয়ে দিয়ে দেয়

BEEF XSS

---

so যাতে না করতে পারে তাই

⇒ Post explotation

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Table 1.3 Security Mechanisms

Pervasive = General.

IDS = Intrusion Detection System

↓

event detection

IPS = Intrusion Prevention System

↓

Firewall

Event viewer

↓

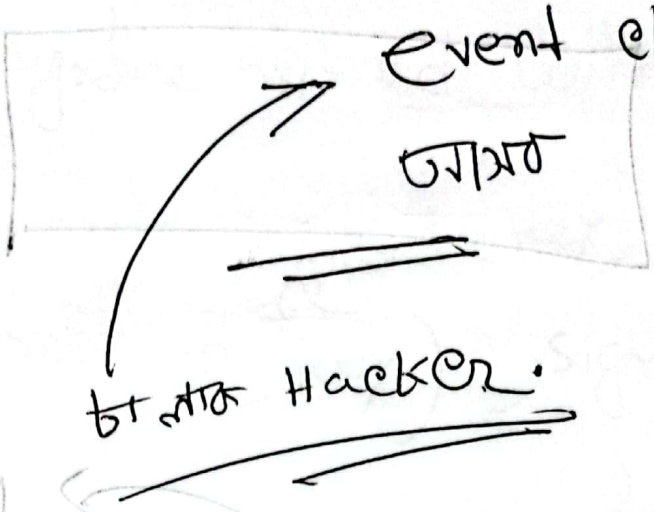
windows log.

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

/var/log/syslog



- Security Auditing / penetration Testing

Third party

Security Audit Trail.

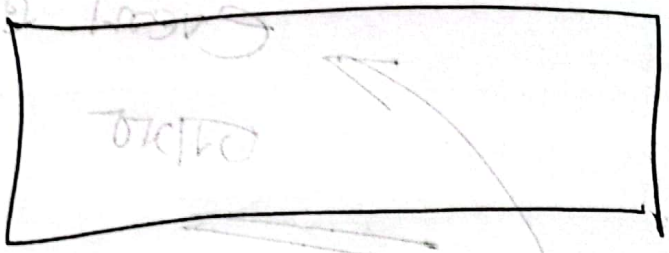
Paper work must be.

Pervasive security mechanism.

Cipher = encryption algorithm.

Theme: Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri



Digital signature

What is digital signature?

validity

verification

Reverse Process

if verification Pass then it's Real.

if fail then it is not real.

String of data 0's and 1.

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Digital signature append with actual msg.

Sign (message, key) = signature (private key)

verify (signature, public key) = m

Foxit Pdf

Protect

↓

Add id

↓

Digital certificate

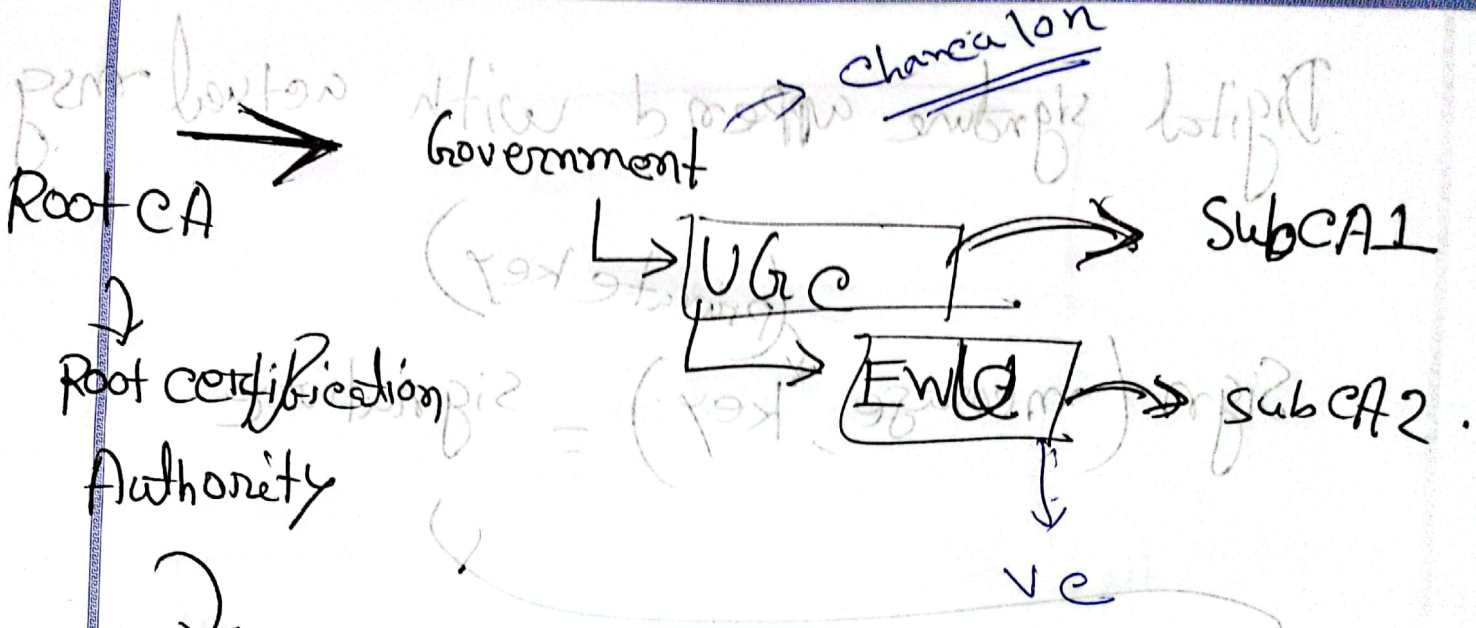
Trust is a digital object

It can be Transfer.

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri



Theme: Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

self sign certificate

↓

is valid

Trust is a digital object

and it is chain.

CSR = certificate signing Request

↓

certificate নিজেই বানাব,

Then Root certification authority র কাছে পাঠাব,

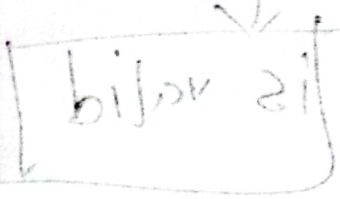
Digicert → paid করা most 600+ dollar.

→ তারা অনেক সব check করে,

→ brand value.

let's encrypt → ফ্রিতে দিবে (Domain only validated)

Certificate Hierarchy



Digicert

/apache.conf → Facebook.com

SHA-256

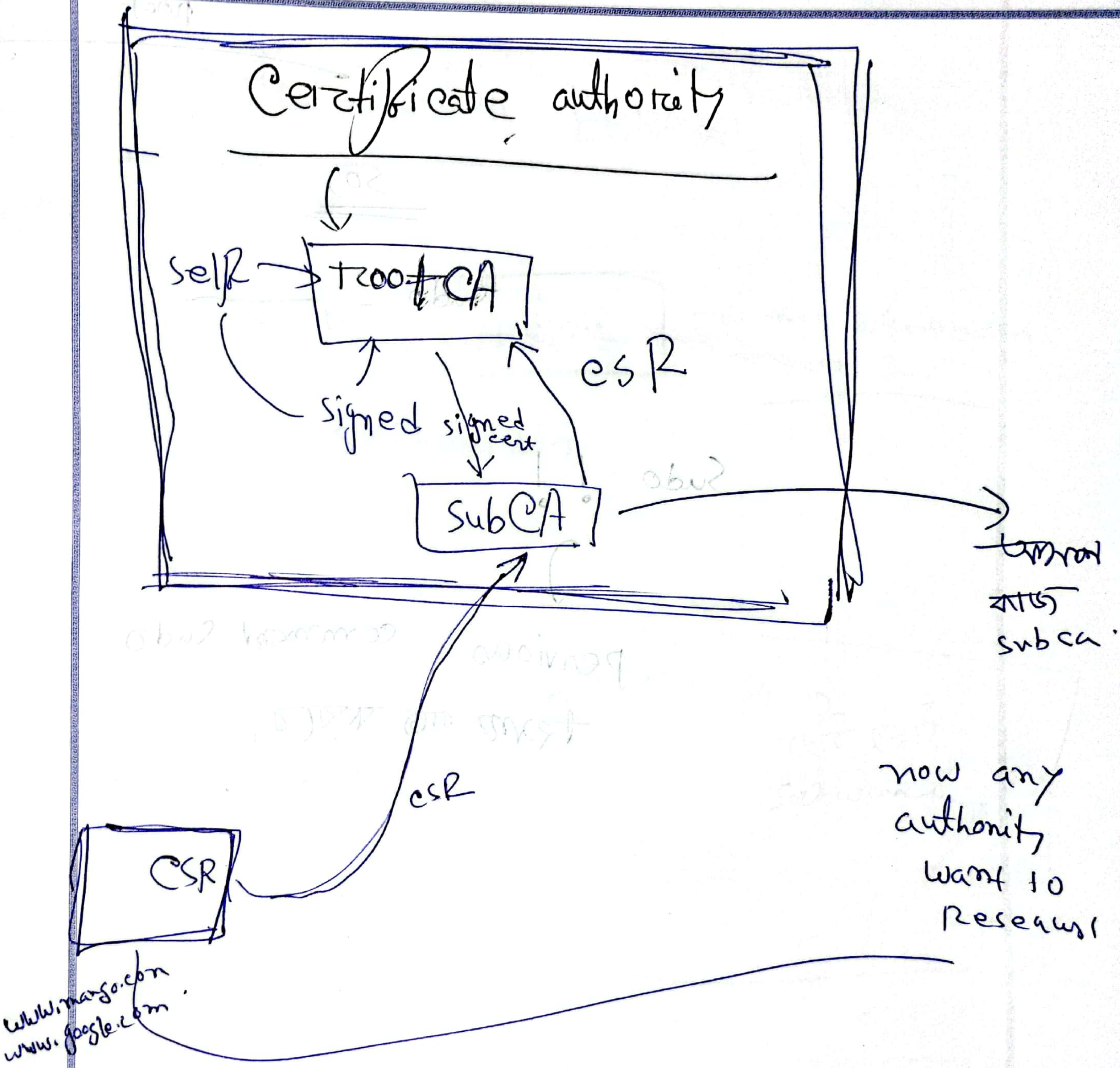
Fingerprints

↓

integrity ensure.

Theme: Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri



/var/certs/* .cert

Make sure Apache HTTP or Nginix user not be root other wise make মাটি হবে।

eme:

Date: /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

sudo su → Permanently root

SO;

Sudo

Sudo !!

↓

pervious command sudo

দিয়ে রান করাবে।

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Authentication Echange

SAML / OAuth2 → open authentication version 2.

Shibboleth

Rasbery Pi কে ছোট ছোট software

raw code.

Notanization → সত্যায়িত করে।

→ Fourth edition

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Model for Network security.

Opponent ≥ means Hacker.

OWASP TOP 10

↓

your product must Hack by top this top 2021 list to reason

1/11/23

Trust can be shareable

Shared secrect

Notarize

paid ... ISRG

... Domain ...

paid ... Digicert

Standard

MTB Bank

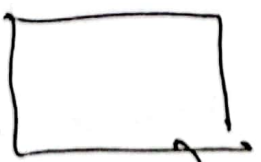
UCB Bank

600 dollar 7ear

facebook

paypal.

...company.



search

Attack surface (SQL injection)

7, root us...

Attack surface Category

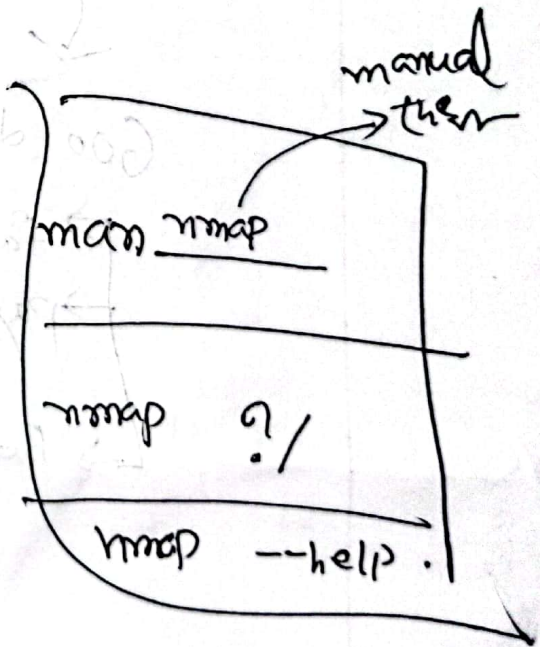
- Human Attack surface → মানুষ কেন্দ্রিক আক্রমণ
- Network " "
- Software " "

---

port scan

nmap
(
Linux

zenmap ↓
GUI.



(2)

Port
0–1023
↓
reserve port/or well known port

5900 Vne=virtual networking card

Sudo apt-cache search ssh
↓
terminal

22 ssh
↓
secure shell.
↓
Remote login

sudo apt install Openssh

sudo yum ;intsal Openssh
↓
CentOS, RedHat

sudo Packman install.

23 telnet
↓
not secure.
↓
kind of ssh

nmap ইন্সটল করার tutorial

Windows > notepad ./hello.txt.txt

↓

textediton

open port means unathorized access

Linux > sudo nanow hello.txt .

softwarename

. Sudo gedit hello.txt

Vim

Xubuntu Leafpad

↓

kali linux

lubuntu mousepad

Sudo su

↓

যখন না না

তখন Run as administrator

করব

dangerous

X

Aptach-e virtual host wikipedia. (3)

↓

name based vs Ip based

→ williamstallings

→ web scraping

ATtack Tree → ewu portal

↓

Bkash APP

Question on exam

Network Attack

software Attack

human Attack

page - 38

Attack Tree

page → 40

Model for Network

URL Parameter Hijacking

Oppset = reactor = Attacker

=

Security Standard

NIST, Internet Security, ITU-T, ISO, .

RIP, OSPF

interior protocol.

~~ভিতরে~~ কাজ করে
organisation
এর ভিতরে,
(subnet এর ভিতরে)

AS Number

BGP ⇒
Border Gateway Protocol.

vlan [virtual lan]

Atonomous

Exterior gateway
protocol
↓
BGP.

AS number — organization identify.

East west University ASN.

↓ Google search.

↓ Autonomous System.

William Stallings

↓

[illegible]

3 [illegible]

[illegible]

[illegible]

ceaser cipher — Rot13

↓

13 ঘর সামনে encryption

↓

classical encryption algorithm

↓

এখন আর use হয় না

↓

Neso academy → ওদের math বোঝাবে

↓

youtube.

4500

slide 2 shared folder

Execution in a function

William Stallings Network security essentials Online class

Theme: Chapter-2

5 11

Date: 10 / 5 / 23

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

greenbar SSL

$E(m, key) = c$

$D(c, key) = m$

$E(m+3) = c$

$D(c-3) = m$

To same key

then Symmetric Encryption

key = key

encryption, Decryption

same key

Encryption key = Decryption key

scam

symmetric key cryptography

Private

sender receiver

A → B

key = 3

key = 3

Asymmetric key cryptography

Encryption key ≠ Decryption key

Public key Cryptography

Theme:

Date: ☐Sat ☐Sun ☐Mon ☐Tue ☐Wed ☐Thu ☐Fri

Alice (A) keypairA

only owner
Privatekey

Publickey

Bob (B) keypairB

only owner
Privatekey

Publickey

$E(m, PvtA) = C$ → Private

$D(C, PubA) = m$ → Public

lock

unlock

Alice নিজের only কথা হচ্ছে

Public

$E(m, PubA) = C$

$D(C, PvtA) = m$

একটা দিয়ে encrypt করলে আরেকটা দিয়ে decrypt.

Algorithm must be open.

Private key Public key mathmatically must be linked.

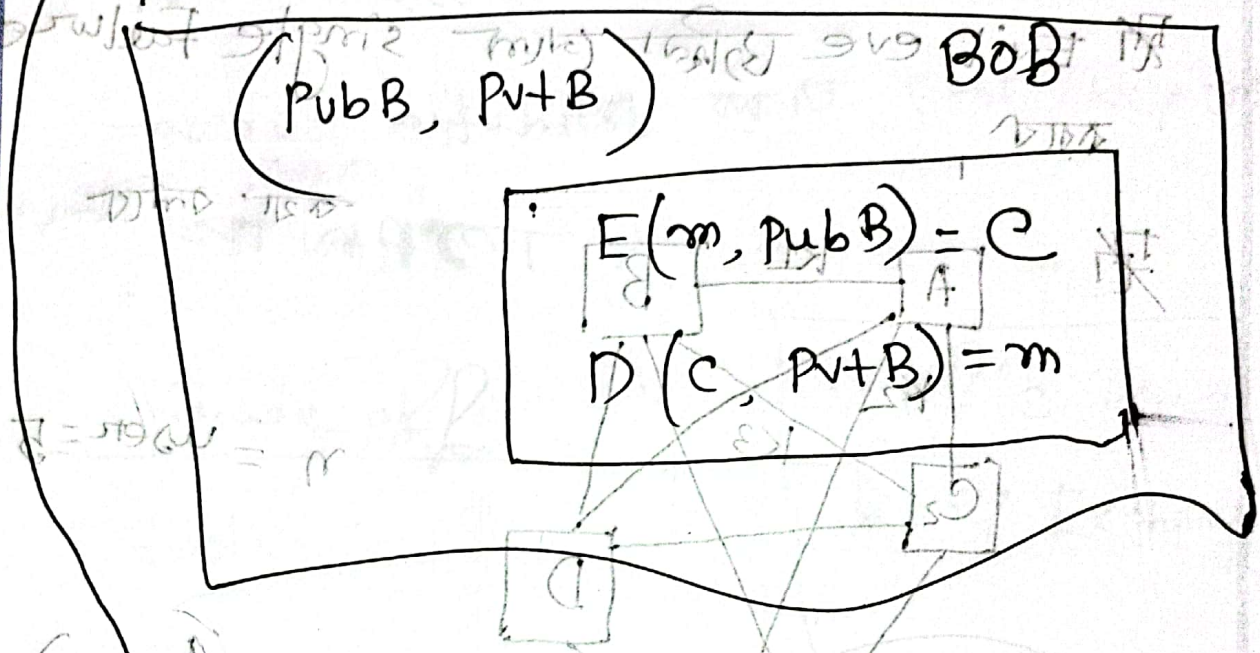
Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

secret key

Key Establishment Problem



What is the problem of symmetric Algorithm ?

$E(m, key) = c$

(E)

(A) c — c — c — c (B)

$D(C, key) = m$

main problem

key value Agree করা

যে geographically possible না

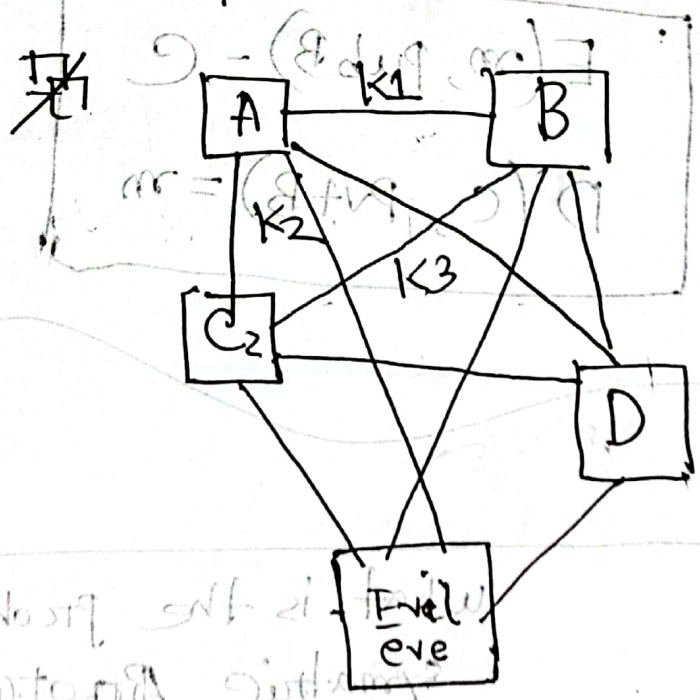
Alice আর Antartica Bob এর America.

Key space ছোট হলে brute force করা যাবে

Theme: symmetric encryption problem Date: / /
□Sat □Sun □Mon □Tue □wed □Thu □Fri

So আরেকটা channel লাগবে

Evil eve থাকলে single failure করবে



কথা বলবে

n = user = 5

$$\frac{n(n-1)}{2}$$

$$= \frac{5(5-1)}{2}$$

$$= \frac{5 \times 4}{2}$$

$$= 10$$

if number of key

If 100 user then

$$\frac{100 \times 99}{2}$$

= number of keys

Theme: Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

so অনেকগুলো password এখানে db maintain করতে হবে।

~~আমরা~~ establish করার জন্য key কে ~~করা~~ ~~এখানে~~ [illegible]

Trade off → Diffie Hellman Key Exchange

Faster

symmetric key

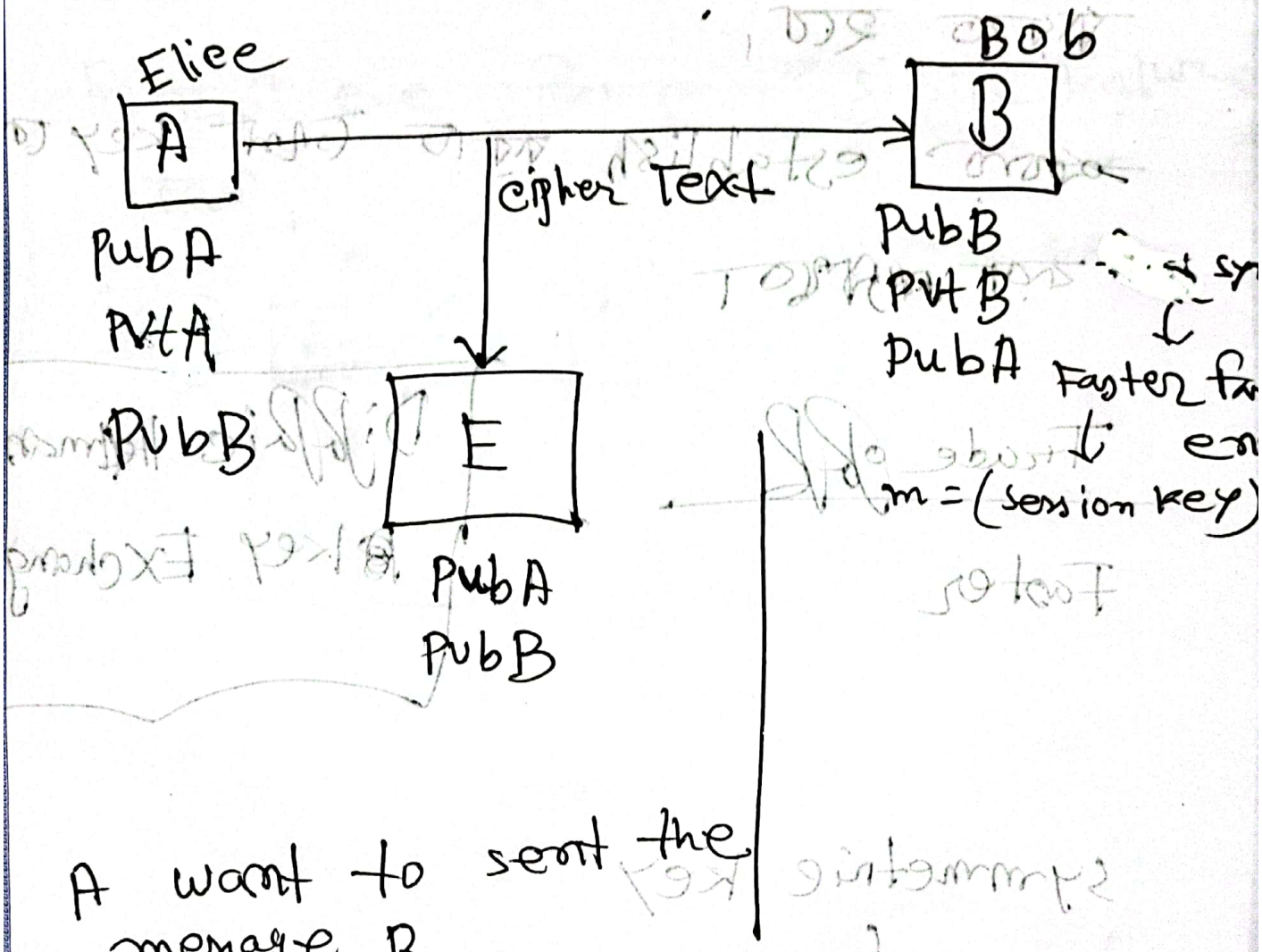
↓

session key (session ~~[illegible]~~ destroy)

---

so First এ session key দিয়ে সবাইকে message পাঠাবে।

m = (session key



A want to sent the message B

$E(m, PubB) = Cipher$

$D(Cipher, PvtB) = m$

vice versa.

Theme: Christof paar Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

understanding cryptography.

book + slide

Basic Transport Protocol

16 page

Protocol

message ~~চালাচালি~~ নিয়ে বুঝাতে হবে.
We are looking at know protocol.

Example hybrid protocol with AES

Assymetric + symmetric

Assymetric key
↓
slower.

Advanced Encryp. Standard.
↓
Symmatric

cryptography

1) the type of operation used for transforming plaintext to ciphertext
2) Number of keys used
3) The way in which plaintext is processed

Figure 2.1 ← William stallings Network security essentials 4th edition

cryptography and Network security 5th edition

Theme: Date: / /

Sat Sun Mon Tue Wed Thu Fri

w. stallings

Cryptoanalysis → Decryption without key use

page → 4th edition William stalling

Network security essentials

chapter - 2

Theme:

Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

Classical encryption Algorithm

- Cisar cipher
- Brute force করা যায়
- xm এর আগে না, যখন চিহ্নিত হয়ে যায়

$$E(m, key) = C$$

m = 0000 01000 | 1111 11000

block

block

key = 1011 0111

block of data নিয়ে কাজ

block cipher

$$E(m \oplus k) = C$$

int ('X') = ASCII (x)

Theme:

Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

$m = 'XOXO'$ (0-255)

8 bit block

$2^8 = 256$

$E(X, key) = C$

$E(O, key) = C$

$E(X, key) = C$

$E(O, key) = C$

Streaming data

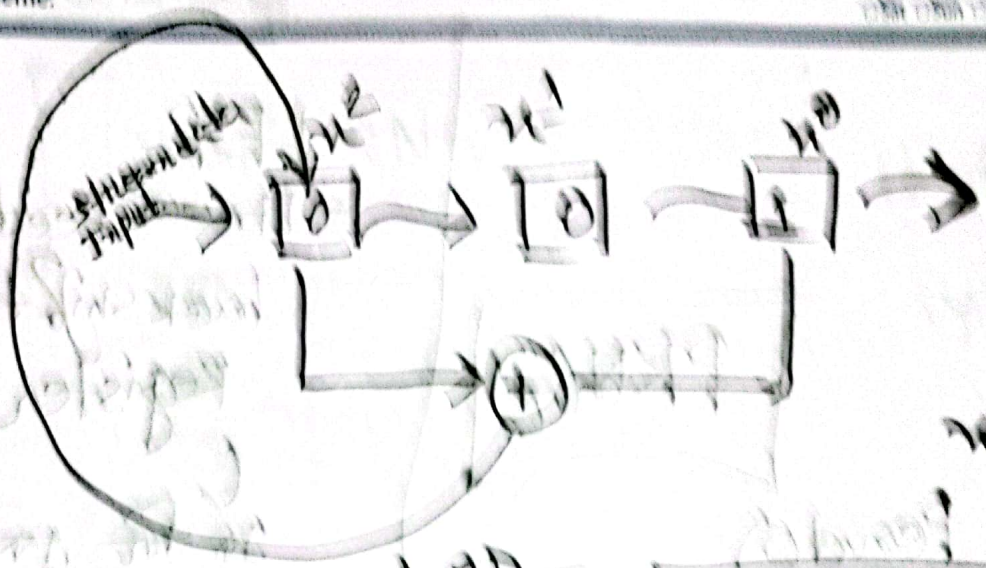
How to Padding

1 bit করে encrypt করে, decrypt করব।

Actually 3 bit করে

হবে।

Theme:



Stream cipher
RC4

Block Encryption
AES, DES

How to Design
secure Encryption
routine,

DES, TDES, 3DES

PRNG
Pseudo Random
Number generator

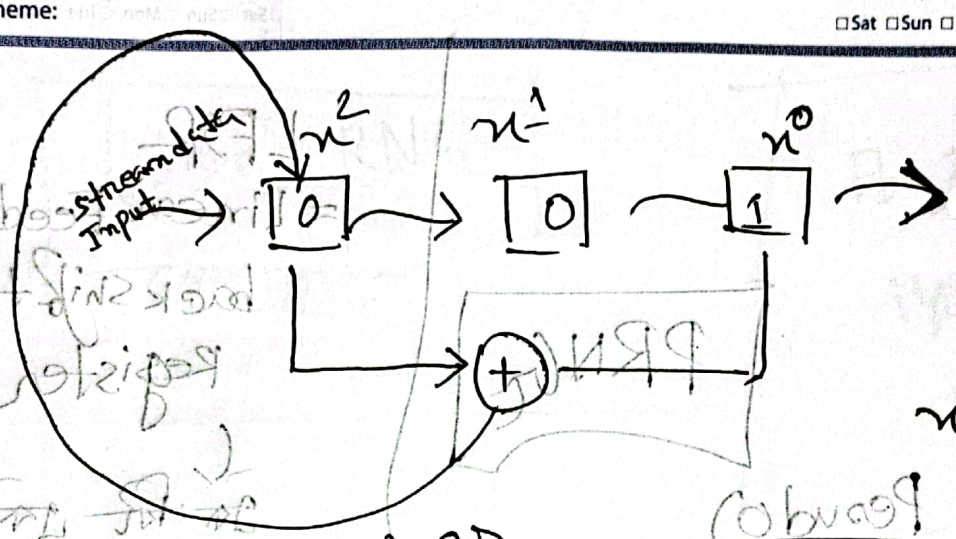
TRNG

True random
number generators

Theme:

Date: 6/11/23

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri



x^2+1

Stream cipher

RC4

key = 1111 0000

8 bit রাখার পর Repeat হবে।

Block Encryption

AES, DES

Data

How to Design secure Encryption youtube.

key = 128 bit key - sequence

PRNG

Pseudo Random Number generator

TRNG

True Random Number generator

DES, 2DES, 3DES

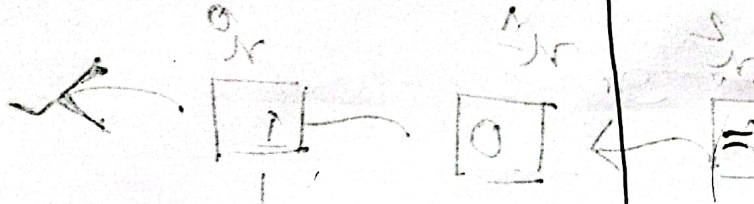
এটা না

এটা

Theme:

Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri



PRNG

(Pesudo) → আসলে না Random এর মতো দেখাত

Fake id.

(Pseudo) RNG

= Seed + Algo.

LFSR

= Linear Feed back Shift Register

↓

এক বিট একটা storage register একটির পর একটি করে যাবে shift হয়।

100100111001110

↓

Hacker কী বোঝে কিছুই বুঝবে না, কিন্তু Alice Bob বুঝবে।

Theme:

Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

(True) RNG

Fb ওয়ালারা typing ওপর ও depend করে data collect করে

যারাই typing pattern

website → Authentication

Auth Token → server দিবে

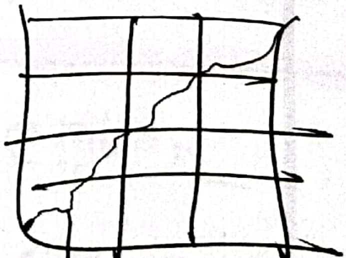
Session Token → communicate করে

Session Hijacking

cookie secure রাখা জরুরি

Captcha

Random



→ Randomness,

session Token দেওয়া ছাড়াও আলাদা কিছু আছে জানতে হইবে, sin on the Record রেখো নাই

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

lightbeam → extention

cookie যেখানে নিজেরার info চালাচালি ও ঘাটাঘাটি করতেছে।

Theme: Class

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Network security essentials

4th edition

cryptography and Network security

5th edition W. Stallings

CODE Book থাকতে হবে

shared secret

2.2 Substitution Techniques

Symmatric Cipher

Replace বসাবে

Caesar cipher

monoalphabatic ciphers

playfain Cipher

Hill cipher

Polyalphabetic ciphers

one Time pad

Alphabet ১টা

A B C D . . . E

P ↓ we

B never use P

If we P then Polyalphabetic

Alphabet ২টা

Theme:

Date:

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Team position Techniques

position ~~[illegible]~~ এ change করে থাকা

ABC party

&

Anything But Clothes

toga party

Greco-Roman theme

Costume party

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Shift Cipher

1. Brute force

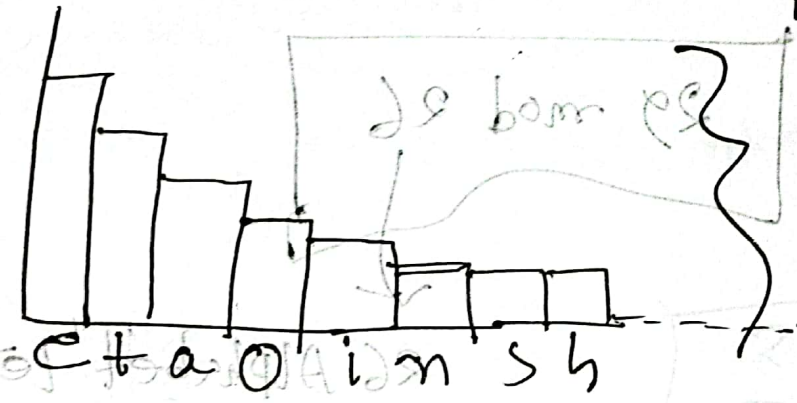
Find the value of the key.

20

2. Crypto Analysis

th qu

pattern



English letter Frequency

word

suppose W সবচেয়ে বেশি বার আসছে

so, W to e হল

18 or

W to e

8

26-8

=18

So যখন character + B value যোগ করতে হবে।

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

$a = 97 \bmod 97 + 1$

$A = (65 \bmod 65) + 1$

$E(m + (-\delta)) = c$

$D(c - (-\delta)) = 5$

$\text{Ord}(A)$

$29 \bmod 26$

26 Alphabet letter.

key 4 3 1 2 5 6 7

a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

Cipher Text TTNAAPTMTSUO

AOWCOIXKNLYPETZ

Theme: Rotor Machine. Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

↓
Encryption Decryption

Network security Essentials 4th (2010)

Blockchaining.

linked list

2.5 page 51

book

CIPHER Block or Mode operation

symmetric key

e. key value

Cipher Text

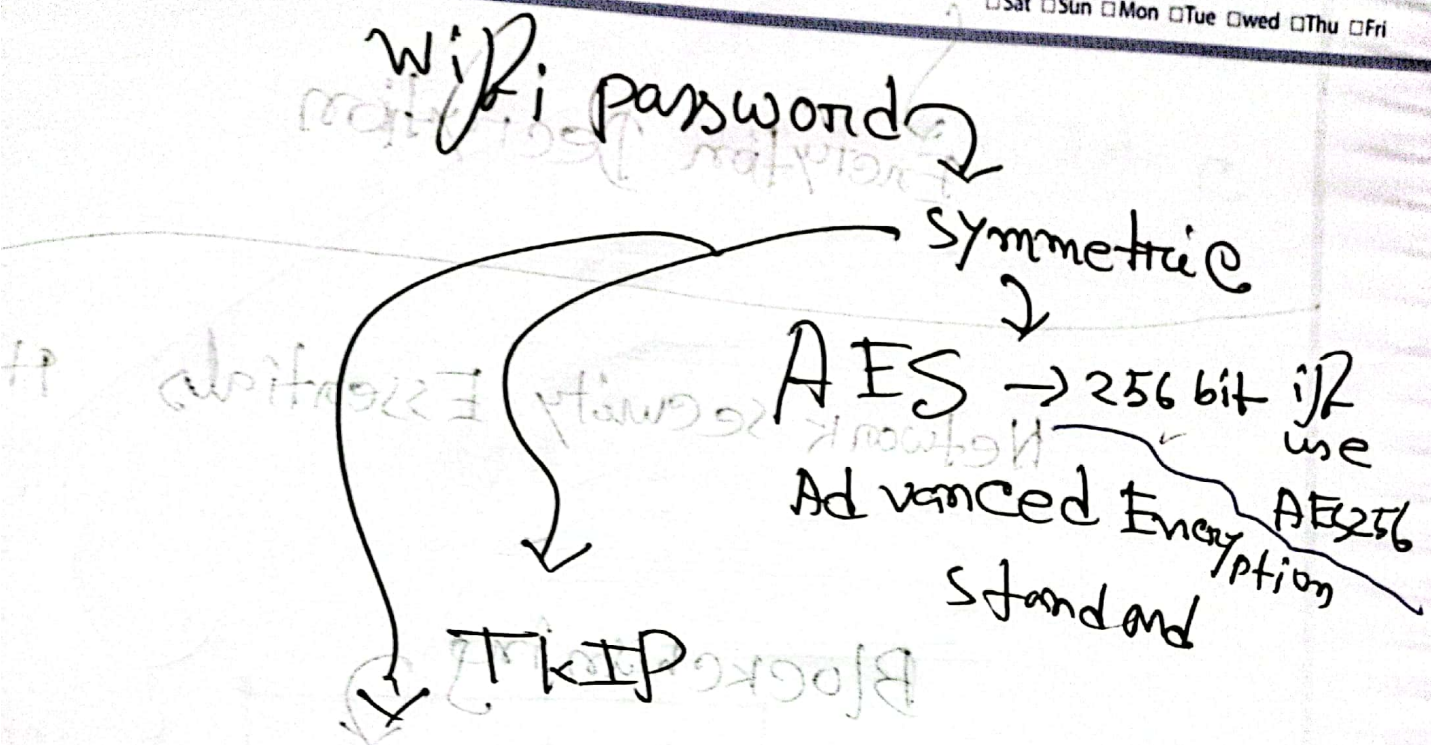
XOR

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Wifi password



বুঝার কোনো Password এমন

---

8 char, 9 char password

brute force (A to Z)(a to z)(0 to 9)

Q. 1000 Password second rate time?

Table → 2.2

a to z = 26	
A to Z = 26	
0 to 10 = 10	
62	

↓ Q

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

$T_8 = \frac{26^8}{1000}$

$T_9 = \frac{26^9}{1000}$

encode decode

base64 to binary

6 bit

$2^6 = 64$

then

(ASCII)

8 bit

$2^8 = 256$

block Cipher

Left side

ডান

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Modular 2 Arithmetic

X-OR

Same – 0

Different – 1

if one or zero

1 + 0 = 1

1 + 1 = 0

0 + 1 = 1

0 + 0 = 0

1101

0101

1000 X-OR

1000

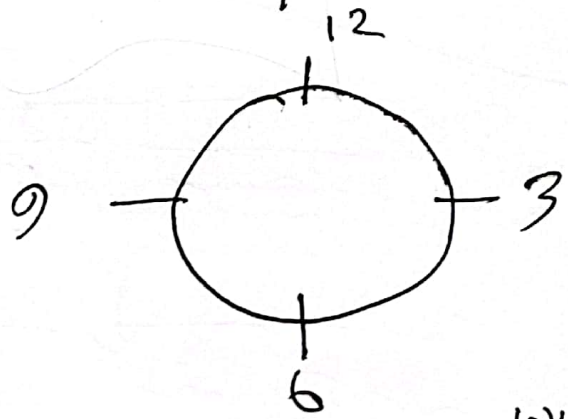
0101

1101 X-OR

যোগ বিয়োগ দুটোই X-OR যোগ

Finite Field Arithmatic

Modulear Arithmatic



13.30 means 1.30

How 13%12 reminder 1

12)13(1
12
1

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

27 means

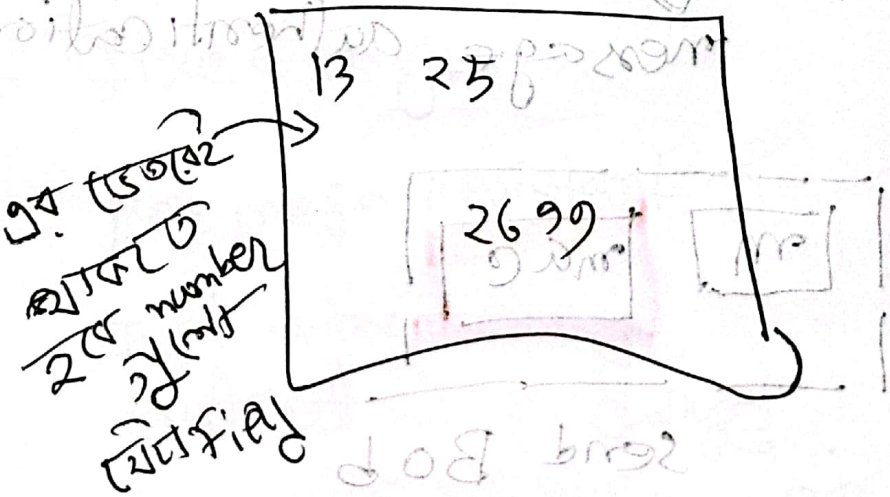
$27 \bmod 12$

12) 27 (2
24
3

3

$$27 \equiv 3 \bmod 12$$

Finite Field Arithmatic.



Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

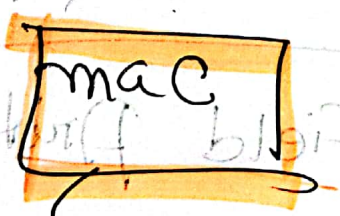
Network security Essentials (ch-4)

Chap – 3

W. stalling.

Public key cryptography

Message Authentication



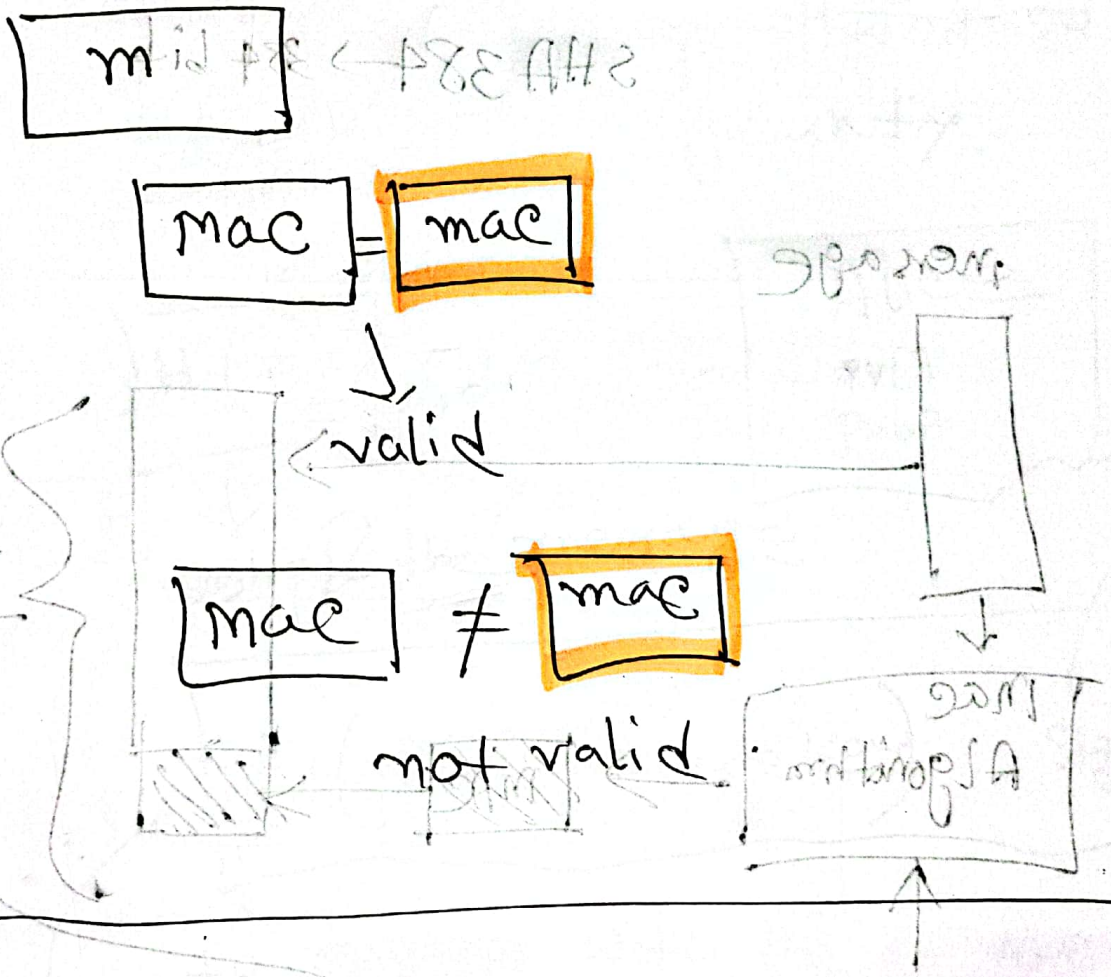
message authentication code.

send Bob

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri



book

what is hash ??

- one way function
- fixed length
- pre image resistant → ধরে করে যাবেনা যা দিছে
- Input minor change
  output mela change.
  Avalange effect

Theme:

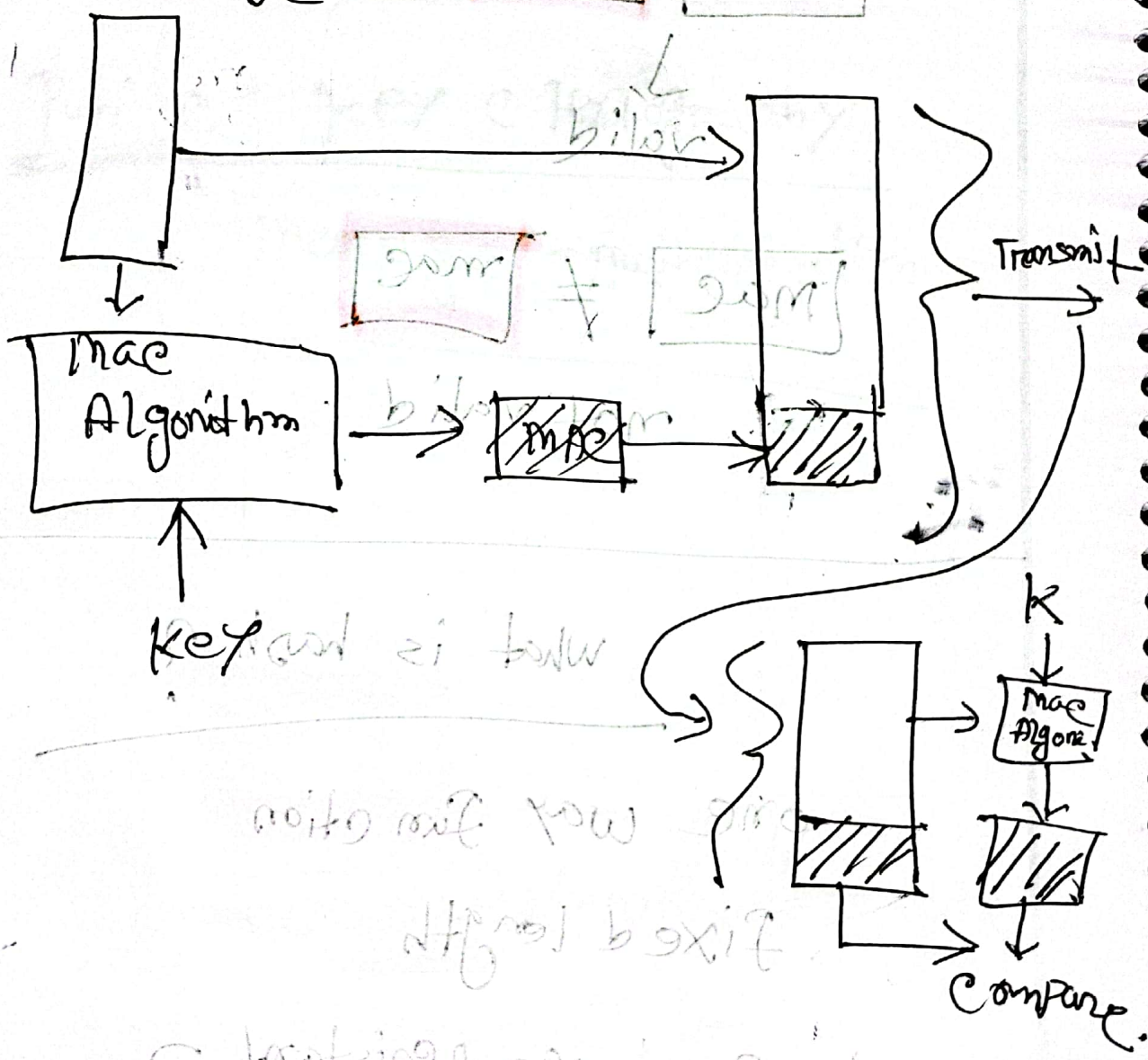
Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

SHA1 → 160 bit

SHA256 – 256 bit

SHA384 → 384 bit



Theme: Date: / /

□Sat □Sun □Mon □Tue □Wed □Thu □Fri

Integrity → message পরিবর্তন হয় নাই garanty.

H (m) → Hash of the message

Alice
PvtA
PubA

This signature is MAC

Sign(H(m), Private key$_A$) = Signature$_A$

to encrypt with the private key of the signer.

to decrypt with the public key of the signer...

sign oposite function verification)

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐T

Signature A

means MAC

Verify (Signature A, PubA) = Verification

H(m)

সবাই জানে

Now Bob Rec

the message valid

same m

also he got m

h(m)

m | MAC

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

How evil eve want to change the message

Sign(H(m), PvtE) = Signature E

Mac

Ver(Signature E, PubA) = h(m)

Alice PubA

h(m) = ~ X

Theme: Date: / /
□Sat □Sun □Mon □Tue □wed □Thu □Fri

message এবং message hash change হলে
for কোনো signature কারণ
Integrity নিয়ে

without

Confiedentiality

essentials Network Security 81 Page

ensure হয় নাকি →

যখন message টা
দেখতে পারে

Un Forgeable
নকল করা

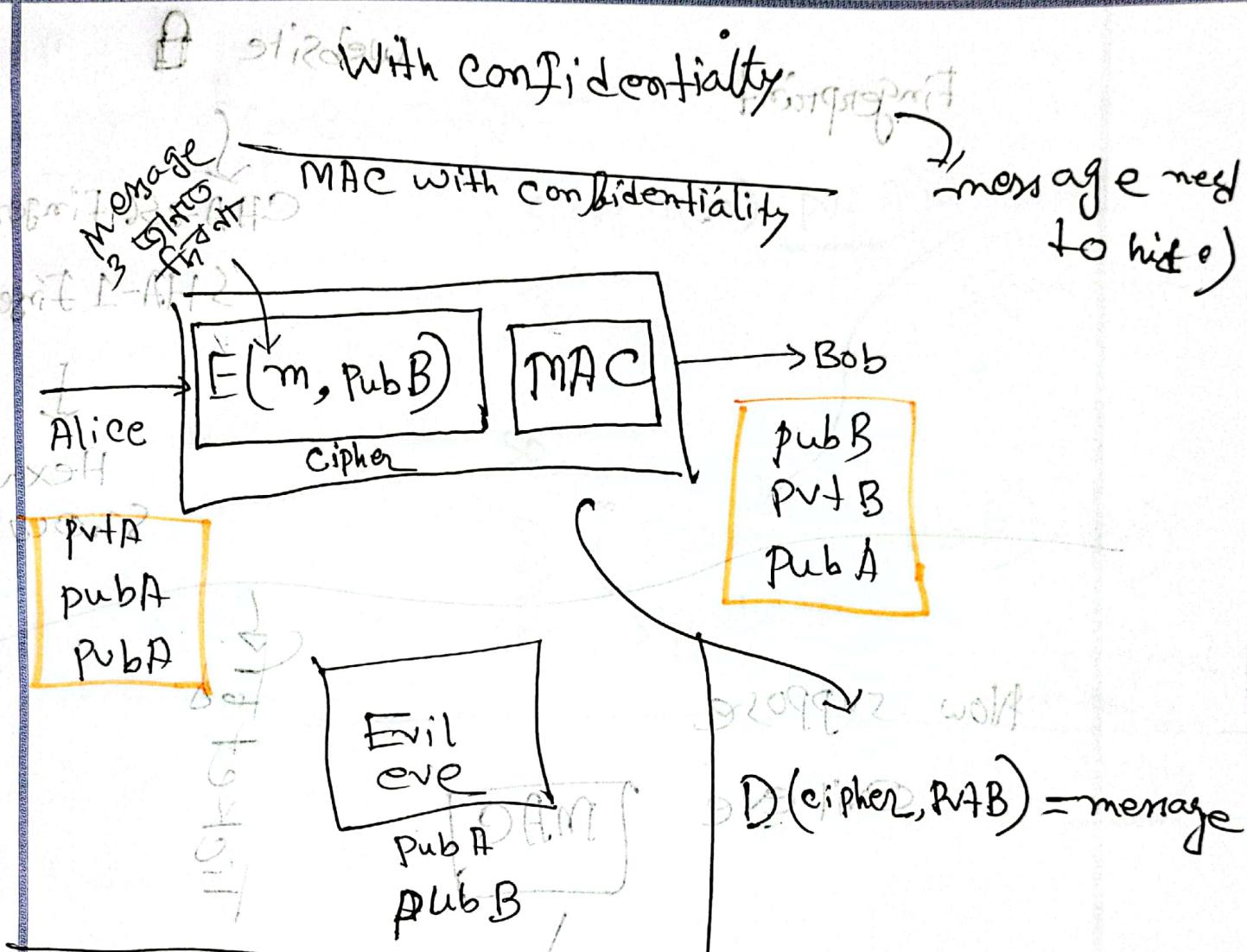
2048 bit number key Public Private

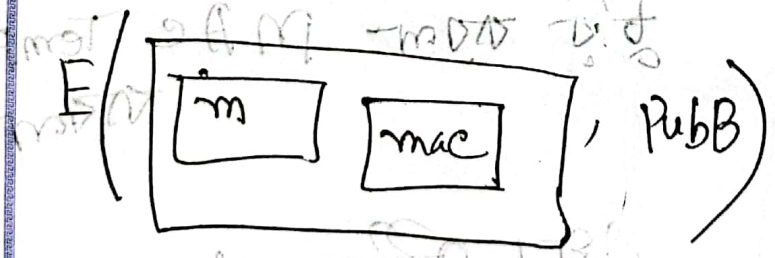
Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

With confidentiality





b = pubB = 2048bit

Base 64

----begin

Publickey----

asdf123afdsfn

----end

Publickey----

sha-256sum (Publickey)

C = SHA256 - Fingerprint

Linux hash function

Hash (publickey)

= Fingerprint

Theme: Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

Fingerprint website 🔒

↓

CHA-256 Fingerprint

SHA-1 Fingerprint

↓

Hex value show

Ticket

Now suppose

Eve

MAC

↓

MAC Temper করল

এখন দুইটা check করব কেমনে

কী জানি

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

MAC মানে

$Sign(H(m), PvtA) = MAC$ on, signatureA

E

So,

$D(MAC, PubA) = h(m)$

ver signatureA

original message

Hash

Theme: Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

K'Khoffs better to use different symmetric key each and every time

Hybrid protocol.

↓

but computational power বেশি।

session অভিবেশন

Zucked ↓ Zuckerburg হালাহার নতুন

Theme:

Date:

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

HMAC = Hash Message Authentication code

AES → confusion

→ Spanning Tree
youtube

→ Diffusion

Page-80

Network security essentials.

4th edition

W. Stalling

RSA, Diffie Hellman

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐Wed ☐Thu

High voltage Provide করে I2C

killer USB

DOS Attack

Time and Remote Tiggering.

মাদারবোর্ড

Denial of services

see the Result computer বন্ধ হয়ে যাবে কিন্তু ধরতে পারব না

Network Security essentials 4th edition

Reply

কোন কিছু নিয়ে অপরিচিত অবস্থায় পরিবর্তন করে আবার ফিরে আসা

masquerade

In Personination means I am donald Trump.

Theme:

Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

Side channel Attack

→ Analysis

দেয়াল ভেদ করে দেখা যায়

wifi router

obstruction

cellular z → sim দিয়ে apk বানাইয়া

Becon signal পাঠাইতে থাকে

ওমুক এত number channel এ connected আছি

কে আমার সাথে connected হতে চাও

Theme: Date: / /
□Sat □Sun □Mon □Tue □wed □Thu □Fri

Generative AI

→ Create new content
(audio, code, images, text, video)

Suppose Room-এ wifi router এবং camera আছে

↓

camera track করে motion এবং picture তুলে Now আমরা জানি যে wifi router wirelessly frequency propagate করে এবং obstraction পেলে change হয় এখন wifi router এবং camera এর data একসাথে train করলাম generative AI দিয়ে তাহলে যদি camera আর router এর info তার

Theme:

Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

এখন generative AI দ্বারা Picture তৈরি করতে পারবে এ নির্দিষ্ট ব্যক্তির যেমনিকার data use করা হয়েছিল। যে ব্যক্তির

AI can 'see' People Through Walls using wifi signals

AI generating Dreams & Turning wifi routers Into Camera to see through Walls

---

The O-RAN Security Architecture

ITU (International Telecommunication Union) X.800

RabbitHole

Theme:

Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri

wikipedia → DOS

Wardriving → ligally

wifi receiver

drive Test

Google maps service improve

wiggle

triangulation.

use করে

Network company

check করে

Network এর তথ্য

আর tower

কোথায় করে

messure করে

mac addres between the location

map between

করে

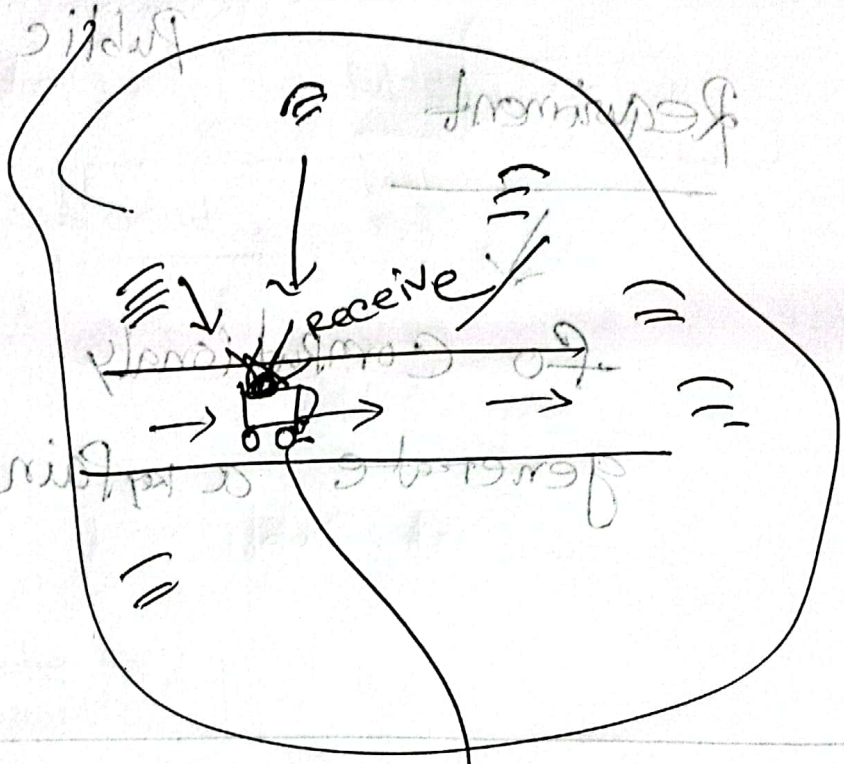
৯.০২৪

আমি তা

Theme:

Date: / /

□Sat □Sun □Mon □Tue □wed □Thu □Fri



Road No and mac address

→ Mac address blur কাকে দেয় যখন কোনকিছু পাঠায়।

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Public key cryptography

Requirment

→ to computationaly easy for generate a key pair (public and private)

OpenSSL → software

- openssl.exe genrsa -out private.pem 2048

Path এক্সপোর্ট দিতে হবে

current folder এ থেকে

openssl.exe

Theme: This pc > Windows(C:) > Openssl > bin

Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Then open cmd this folder

command → Powershell

openssl.exe genrsa -out Private.pem 2048

- openssl.exe → generate rsa
- genrsa → generate rsa
- -out Private.pem → Private key generate
- 2048

Encription algorithm computationally easy.

Decription easy.

Public key জানলে 3 Pvt বের করতে পারবে না,

কিন্তু Pvt জানলে Public key বের করতে পারবে

==
↓
base64 means binary

binary হচ্ছে means Hexadecimal

Theme: Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

RSA → Block cipher
→ Assymmetric
→ developed 1977

↳ Ron Rivest, Adi Shamir, Len Adleman at MIT

First Published 1978.

---

encryption key

$$C = M^e \bmod n$$

decryption key

$$M = C^d \bmod n$$

Important

Predetermined Public number

Finite Field Arithmetic

modular Arithmetic

RSA Algorithm

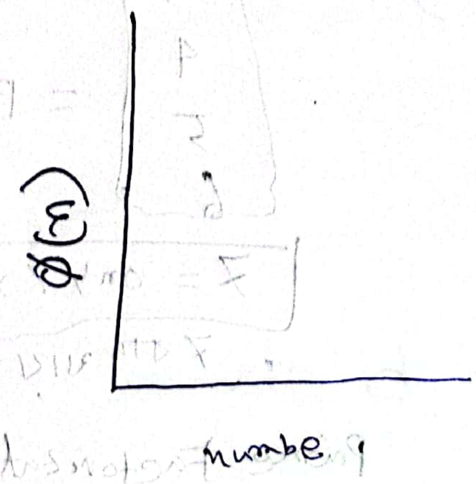
Theme: Date: / / □Sat □Sun □Mon □Tue □wed □Thu □Fri

(Key generation)

RSA based on discreate logarithm problem

Integer Factoring (Prime)

euler's totient function



e*d
?
g mod n

2 = g mod n

2 = 26, 38, 50, 62, 74 mod 12

৭৪ বেশি হবে

n = 8

Phi(8) =
1
2
3
X 4 = 2*2
5
X 6 = 3*2
7
X 8 = Prime factorization = 2*2*2 = 8

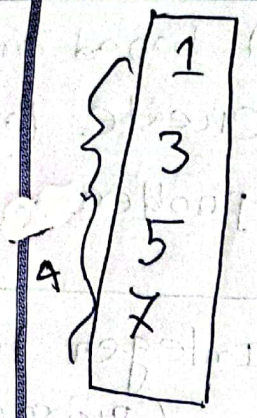
Integer Prime Factorization

2 অবশ্যই বাদে হবে

৪কে ২ দ্বারা ভাগ করা যায়
এখন যে number গুলো
২ দ্বারা ভাগ যায় সব বাদ দিব

Theme: length

Date: ☐Sat ☐Sun ☐Mon



Phi (8) = 4

Phi(7) = 1 2 3 4 5 6 = Phi(7) = 6

7 = only 7 x 1

7 বার যায়

Prime Factorization

$\phi(13) = 12$

only $13 \times 1 = 13$

2

বার যাবে only 13

$\phi(5) = 4$

Phi (any prime number) =

Phi (prime) = Prime − 1

পুরো বারে বাকি সব Just −1 করবে.

Phi (a * b) = phi (a) * phi (b)

Phi (91) = $7 \times 13 = 91$

Phi(13) = Phi(7)

Phi(7) * phi(13)

$= 6 \times 12$

$= 72$

Phi(13) = Phi(7) = 6 ... = 72

not take one integer value e

$$\gcd(\phi(n), e) = 1; \quad 1 < e < \phi(n)$$

72 72

1 ছাড়া অন্য কিছু
কমন ভাগ যাবে না।

Calculate d

$$de \bmod \phi(n) = 1$$

72

Public key $KU = \{e, n\}$

Private key $KR = \{d, n\}$

$de \equiv 1 \bmod \phi(n)$

$de - 1 = \phi(n)(n)$

$de = \phi(n) \times V + 1$

select two prime number $p = 17$ $q = 11$

$n = pq = 17 \times 11 = 187$.

$\text{Phi}(17) * \text{Phi}(11)$

$= 16 \times 10$

$= 160$.

$e = 7$

$\gcd(160, 7) = 1$; $1 < 7 < 160$

↓ coprime

$de \bmod 160 = 1$

$?\times 7 \bmod 160 = 1$

$23 \times 7 \bmod 160 = 1$

$\Rightarrow 161 \bmod 160 = 1$

$e = 7$

$d = 23$

pvt $\{d, n\} = \{23, 187\}$

pub $\{e, n\} = \{7, 187\}$

message.

Plaintext $M < n$

↓

If Ascii value 256 then

$256 < n$

different key use Assymmetric

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

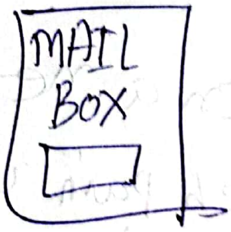
same key use symmetric

Authentication

↓

আপনি যে আপনি প্রমান করবেন

then verification



only owner has the correct key to open the box.

software for encryption and decryption

Eucludian Algorithm

→ cryptography.

→ I/G want learn.

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Symmetic Cryptography problem

1. key distribution problem
   - The Secret key must be transported securely.
2. Number of key, key management.
   - In a network, each pair users requires an individual key.
3. Notarization
   - private key for sign.

key establishment

key management

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Square and Multiply Algorithm

↓ by hand youtube.

$5^{20} \bmod 15$

a^b

binary (20) = 10100 (decimal)

$b_4\ b_3\ b_2\ b_1\ b_0$

b_k

result = 1

for each i from k to 0:

result = $(\text{result})^2 \bmod n$

If $b_i = 1$:

result = $(\text{result} \times a) \bmod n$

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Diffie Hellman key exchange

What is secret key.

Symmetric key

$26 \bmod 12 = 2$

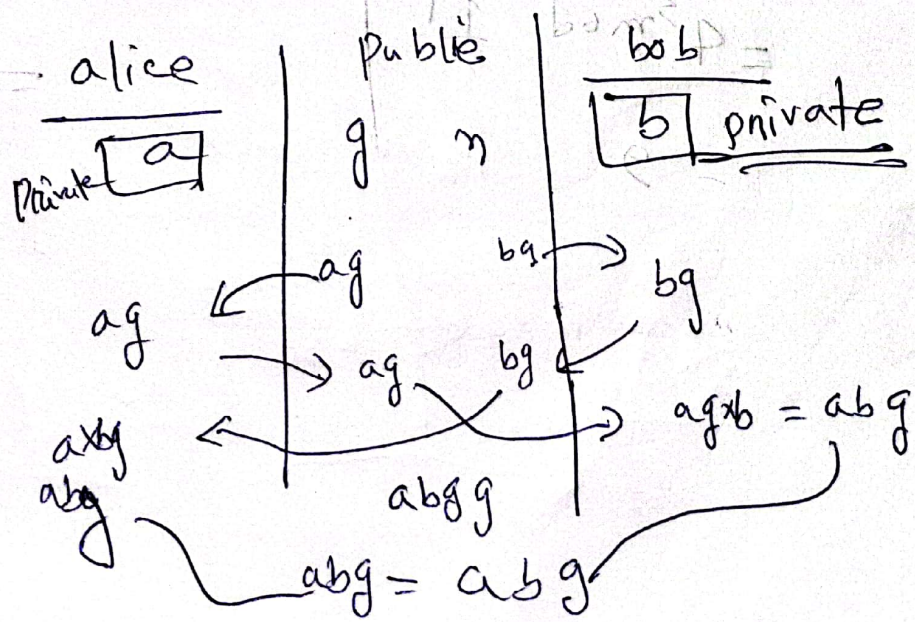
$(26 \bmod 12) \bmod 12 = 2$

$12) 2 (0$

2

University of Nottingham

Dr. Mike Pound



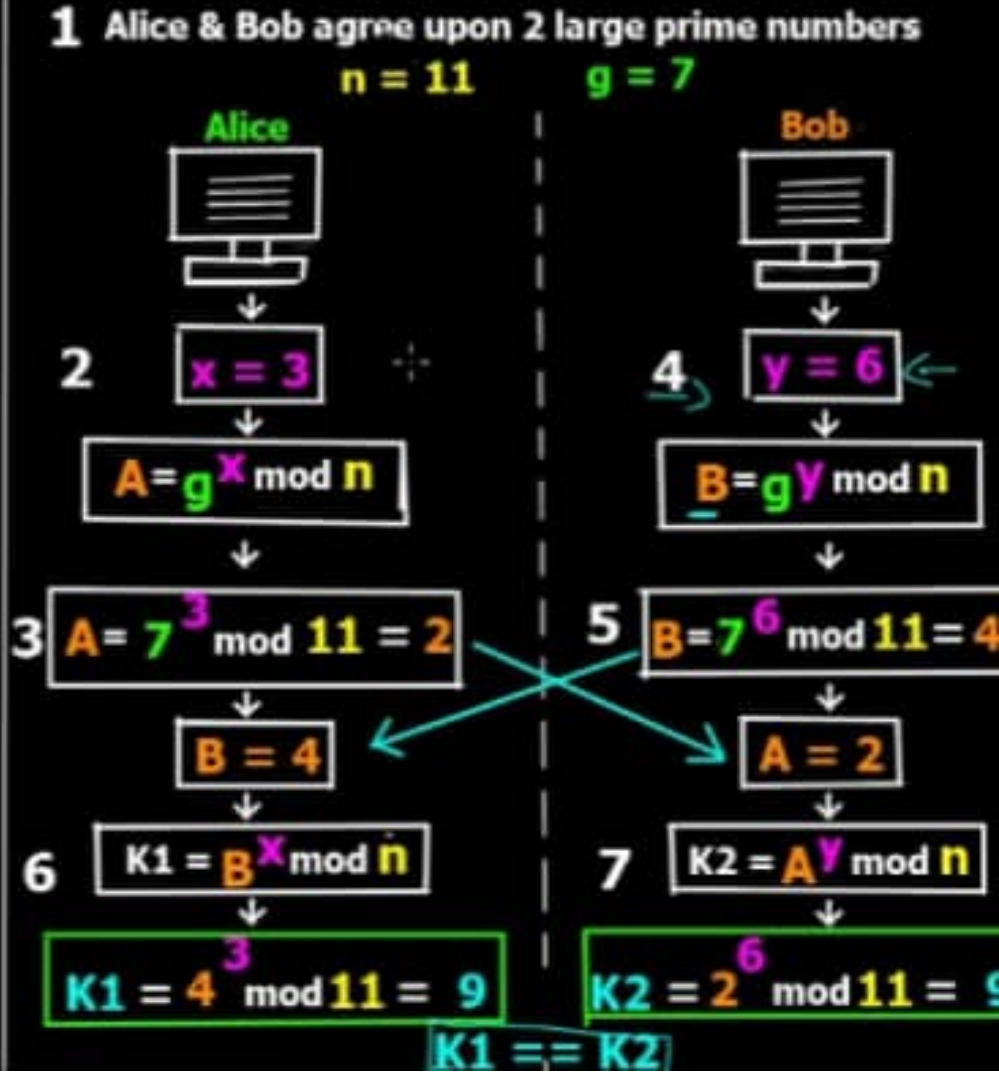
Diffie-Hellman Key Exchange Agreement/Algorithm

Diffie-Hellman Key Exchange/Agreement Algorithm

>> Two parties, can agree on a symmetric key using this technique.
>> This can then be used for encryption/ decryption.
>> This algorithm can be used only for key agreement, but not for encryption or decryption.
>> It is based on mathematical principles.

Algorithm -

1. Firstly Alice & Bob agree upon 2 large prime numbers - n & g
   These 2 numbers need not be secret & can be shared publicly.
2. Alice chooses another large random number x(private to her) & calcuates A such that : $A = g^x \bmod n$
3. Alice sends this to Bob.
4. Bob chooses another large random number y(private to him) & calcuates B such that : $B = g^y \bmod n$
5. Bob sends this to Alice.
6. Alice now computes her secret key K1 as follows:
   $K1 = B^x \bmod n$
7. Bob computes his secret key K2 as follows:
   $K2 = A^y \bmod n$
8. K1 = K2 (key exchange complete)



Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

$n=11$ $g=7$ — public

Alice	Bob
$X=3$ private	$Y=6$ private
$A = g^x \bmod n$	$B = g^y \bmod n$
$A = 7^3 \bmod 11$	$B = 7^6 \bmod 11$
$A = 2$	$= 4$
$K_1 = B^x \bmod n$	$K_2 = A^y \bmod n$
$= 4^3 \bmod 11$	$K_2 = 2^6 \bmod 11$
$= 9$	$= 9.$

Public

Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Theme:

Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Bob

Y=6 → private

$= g^y \bmod n$

$= x^6 \bmod 11$

4

$= A^y \bmod n$

$= 2^6 \bmod 11$

$= 9.$

Discreate logarithm problem (Hard problem)

Integer Factoring (prime factor) Hard problem

PN (Pseudo-noise) sequences

Theme:

Date: /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Side Channel Attack

cryptography

- → Discreate Logarithm Problem
- → Integer Factoring (Prime)
- → ECC (Elliptic Curve cryptography)

what is ECC?

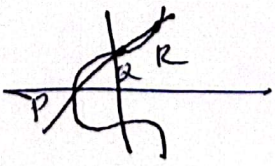
Algorithm Faster

↓

Low Processpower

NIST ECC Graph

Quite standard



$y = x^3 + ax + b$

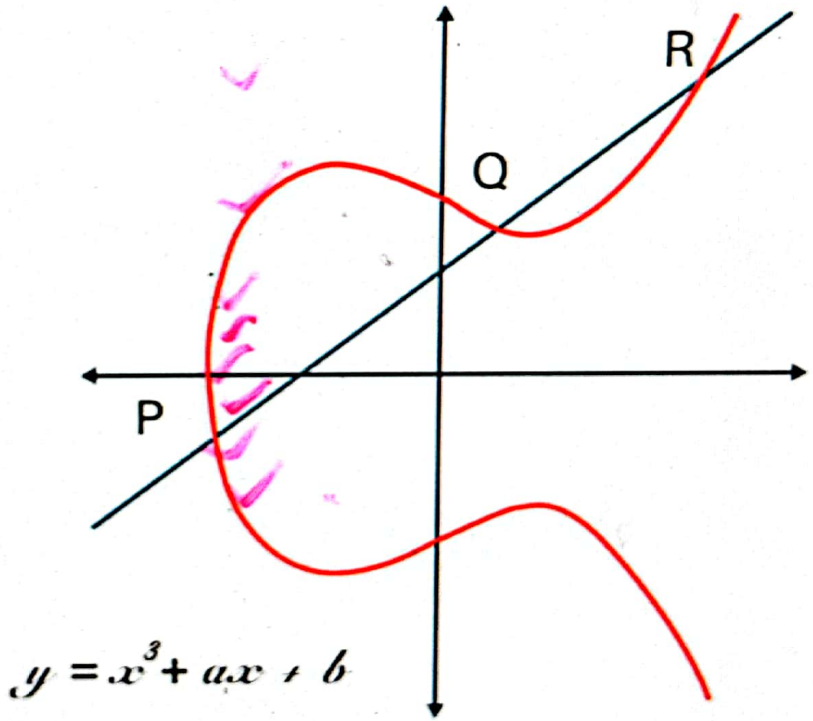
euromancer.sk

graph

Elliptic Curve Cryptography Definition

Elliptic Curve Cryptography (ECC) is a key-based technique for encrypting data. ECC focuses on pairs of public and private keys for decryption and encryption of web traffic.

ECC is frequently discussed in the context of the Rivest–Shamir–Adleman (RSA) cryptographic algorithm. RSA achieves one-way encryption of things like emails, data, and software using prime factorization.



FAQs

What is Elliptic Curve Cryptography?

FAQs

What is Elliptic Curve Cryptography?

ECC, an alternative technique to RSA, is a powerful cryptography approach. It generates security between key pairs for public key encryption by using the mathematics of elliptic curves.

RSA does something similar with prime numbers instead of elliptic curves, but ECC has gradually been growing in popularity recently due to its smaller key size and ability to maintain security. This trend will probably continue as the demand on devices to remain secure increases due to the size of keys growing, drawing on scarce mobile resources. This is why it is so important to understand elliptic curve cryptography in context.

In contrast to RSA, ECC bases its approach to public key cryptographic systems on how elliptic curves are structured algebraically over finite fields. Therefore, ECC creates keys that are more difficult, mathematically, to crack. For this reason, ECC is considered to be the next generation implementation of public key cryptography and more secure than RSA.

It also makes sense to adopt ECC to maintain high levels of both performance and security. That's because ECC is increasingly in wider use as websites strive for greater online security in customer data and greater mobile optimization, simultaneously. More sites using ECC to secure data means a greater need for this kind of quick guide to elliptic curve cryptography.

An elliptic curve for current ECC purposes is a plane curve over a finite field which is made up of the points satisfying the equation:
$y^2=x^3 + ax + b$.

In this elliptic curve cryptography example, any point on the curve can be mirrored over

elliptic curve cryptography.

An elliptic curve for current ECC purposes is a plane curve over a finite field which is made up of the points satisfying the equation:
$y^2 = x^3 + ax + b$.

In this elliptic curve cryptography example, any point on the curve can be mirrored over the x-axis and the curve will stay the same. Any non-vertical line will intersect the curve in three places or fewer.

Elliptic Curve Cryptography vs RSA

The difference in size to security yield between RSA and ECC encryption keys is notable. The table below shows the sizes of keys needed to provide the same level of security. In other words, an elliptic curve cryptography key of 384 bit achieves the same level of security as an RSA of 7680 bit.

RSA Key Length (bit)
1024
2048
3072
7680
15360

ECC Key Length (bit)
160
224
256
384
521

There is no linear relationship between the sizes of ECC keys and RSA keys. That is, an RSA key size that is twice as big does not translate into an ECC key size that's doubled

ECC Key Length (bit)
160
224
256
384
521

There is no linear relationship between the sizes of ECC keys and RSA keys. That is, an RSA key size that is twice as big does not translate into an ECC key size that's doubled. This compelling difference shows that ECC key generation and signing are substantially quicker than for RSA, and also that ECC uses less memory than does RSA..

Also, unlike in RSA, where both are integers, in ECC the private and public keys are not equally exchangeable. Instead, in ECC the public key is a point on the curve, while the private key is still an integer.

A quick comparison of the advantages and disadvantages of ECC and RSA algorithms looks like this:

ECC features smaller ciphertexts, keys, and signatures, and faster generation of keys and signatures. Its decryption and encryption speeds are moderately fast. ECC enables lower latency than inverse throughout by computing signatures in two stages. ECC features strong protocols for authenticated key exchange and support for the tech is strong.

The main disadvantage of ECC is that it isn't easy to securely implement. Compared to RSA, which is much simpler on both the verification and encryption sides, ECC is a steeper learning curve and a bit slower for accumulating actionable results.

However, the disadvantages of RSA catch up with you soon. Key generation is slow with RSA, and so is decryption and signing, which aren't always that easy to implement securely.

Advantages of Elliptic Curve Cryptography

The main disadvantage of ECC is that it isn't easy to securely implement. Compared to RSA, which is much simpler on both the verification and encryption sides, ECC is a steeper learning curve and a bit slower for accumulating actionable results.

However, the disadvantages of RSA catch up with you soon. Key generation is slow with RSA, and so is decryption and signing, which aren't always that easy to implement securely.

Advantages of Elliptic Curve Cryptography

Public-key cryptography works using algorithms that are easy to process in one direction and difficult to process in the reverse direction. For example, RSA relies on the fact that multiplying prime numbers to get a larger number is easy, while factoring huge numbers back to the original primes is much more difficult.

However, to remain secure, RSA needs keys that are 2048 bits or longer. This makes the process slow, and it also means that key size is important.

Size is a serious advantage of elliptic curve cryptography, because it translates into more power for smaller, mobile devices. It's far simpler and requires less energy to factor than it is to solve for an elliptic curve discrete logarithm, so for two keys of the same size, RSA's factoring encryption is more vulnerable.

Using ECC, you can achieve the same security level using smaller keys. In a world where mobile devices must do more and more cryptography with less computational power, ECC offers high security with faster, shorter keys compared to RSA.

How Secure is Elliptic Curve Cryptography?

more power for smaller, mobile devices. It's far simpler and [illegible] factor than it is to solve for an elliptic curve discrete logarithm, so for two keys of the same size, RSA's factoring encryption is more vulnerable.

Using ECC, you can achieve the same security level using smaller keys. In a world where mobile devices must do more and more cryptography with less computational power, ECC offers high security with faster, shorter keys compared to RSA.

How Secure is Elliptic Curve Cryptography?

There are several potential vulnerabilities to elliptic curve cryptography, including side-channel attacks and twist-security attacks. Both types aim to invalidate the ECC's security for private keys.

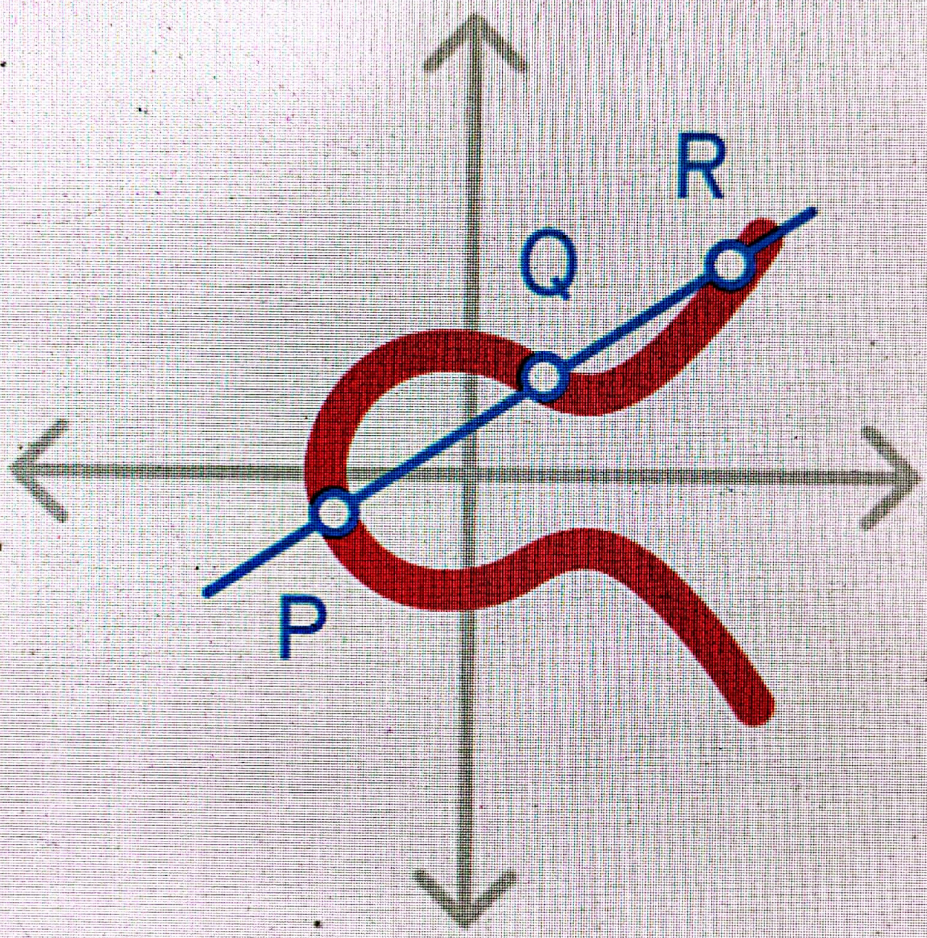
Side-channel attacks including differential power attacks, fault analysis, simple power attacks, and simple timing attacks, typically result in information leaks. Simple countermeasures exist for all types of side-channel attacks.

An additional type of elliptic curve attack is the twist-security attack or fault attack. Such attacks may include invalid-curve attacks and small-subgroup attacks, and they may result in the private key of the victim leaking out. Twist-security attacks are typically simply mitigated with careful parameter validation and curve choices.

Although there are certain ways to attack ECC, the advantages of elliptic curve cryptography for wireless security mean it remains a more secure option.

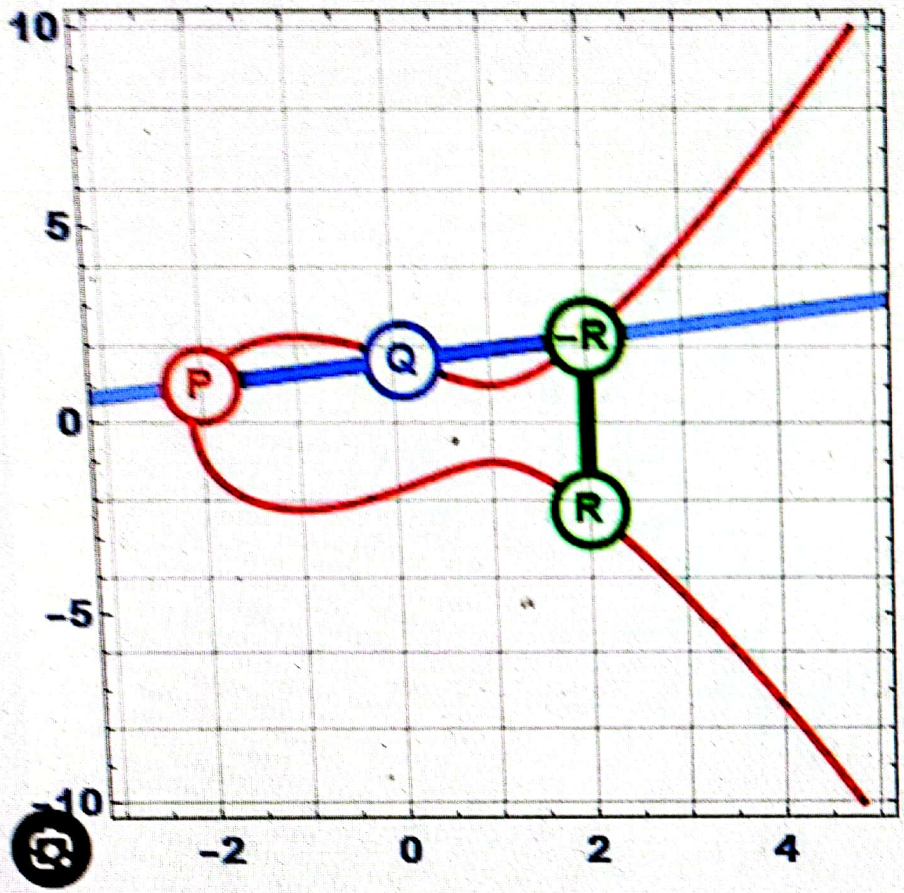
What Is an Elliptic Curve Digital Signature?

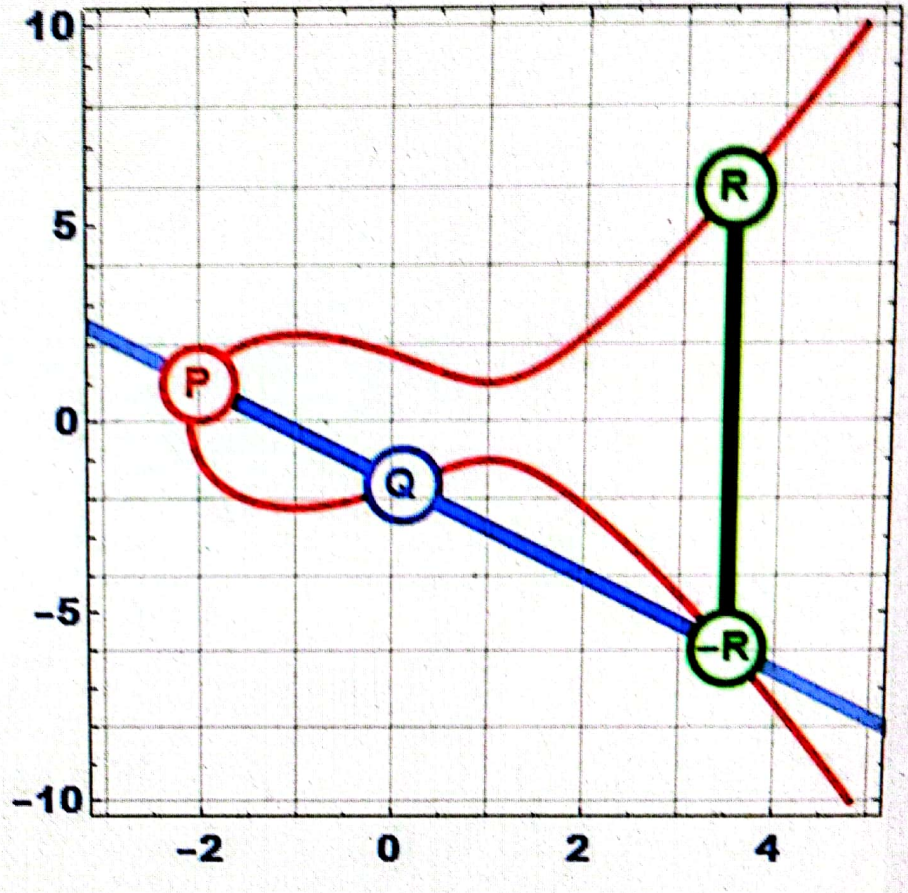
An Elliptic Curve Digital Signature Algorithm (ECDSA) uses ECC keys to ensure each user is unique and every transaction is secure. Although this kind of digital signing algorithm (DSA) offers a functionally indistinguishable outcome as other DSAs, it uses



$$y^2=x^3+ax+b$$

All About Circuits





How Elliptic Curve Cryptography Works - Technical Articles

Visit ›

Images may be subject to copyright. Learn More

Share

Save

Theme:

Date:

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Fork Bomb ২, একটা code যা নিজেকে বারবার Recall করে infinite loop তৈরি করে, Program যা Site কে বারবার কপি করতে করতে entire memory space খরচ করে ফেলবে।

↓ আরো খারাপ না কিছু Try করি।

Hack 5

wifi pineapple

mark VII

Hak5

↓

wireless attack চেয়ার মাঝে লইয়া ঘুরলেই আশে পাশে wifi

Theme:

Date: / /
☐Sat ☐Sun ☐Mon ☐Tue ☐Wed ☐Thu ☐Fri

Drive by Attack

বাস্তব দিয়ে হইটা
যাহিগাড়ি এর মাধ্যে
যদি কোন attack হয়,

Brute force tool: Crunch,
John The Reaper,
Hashcat

Dictionary attack

↓

wordlist

Theme:

Date: C = ooljgt²gs124

Sun Mon Tue Wed Thu Fri

Rock You (linux) → dictionary

decription algorithm dictionary থাকায় গিয়া check করে tutor password বাহির

admIn
h4qr3n
leetspeak

→ so use
amibhatkhi

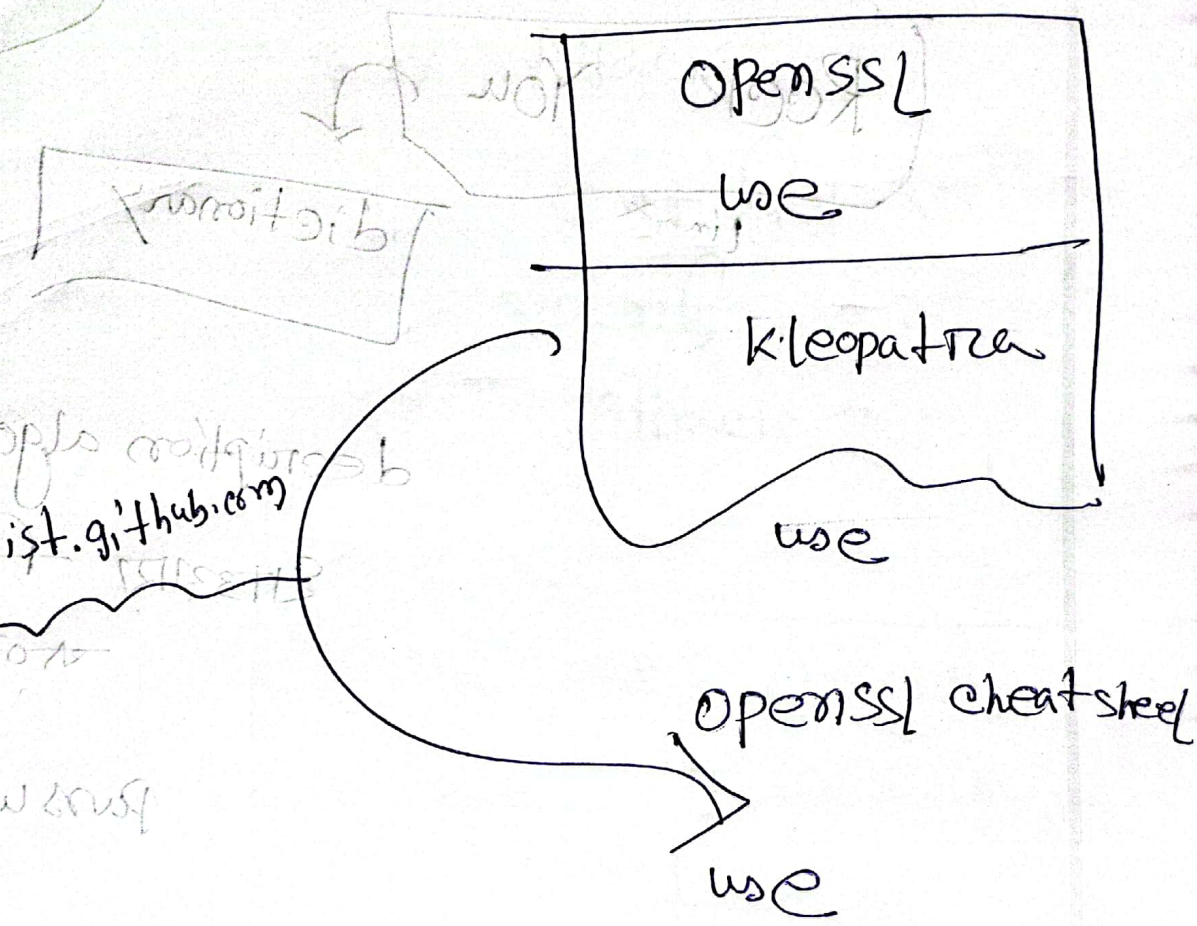
↓

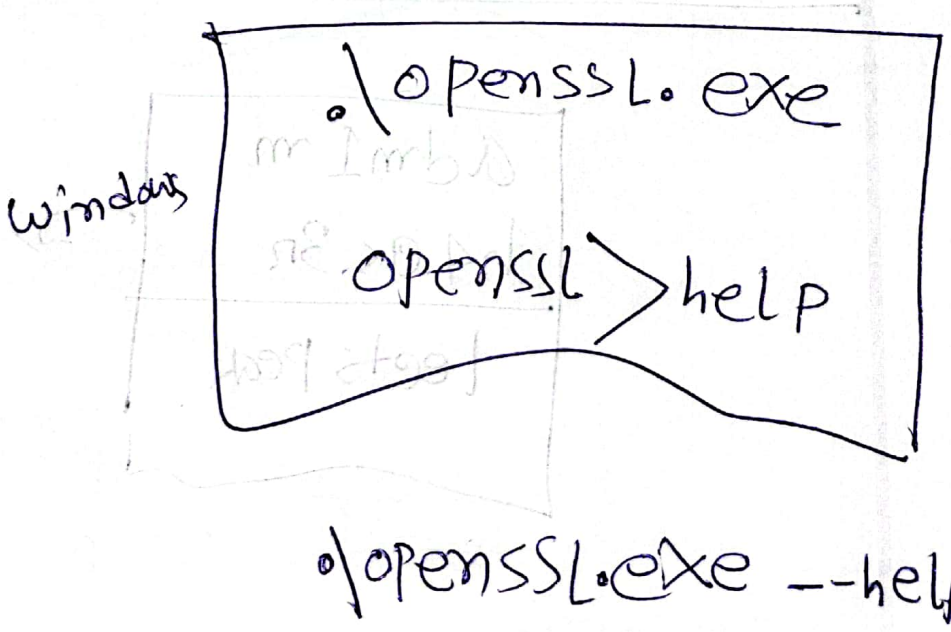
not possible
crypto analytic
to hack

Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri





./openssl.exe --help

Theme:

dh = diffie hellman

dsa = digital signature

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

openSSL command can be aggregated

GoogleDork

Google Hacking Database

GoogleDork private key or Password.

1000 best Google Donks list

gbhacker.com/latest-google-dorks-list/

Find any API key, Password, secret information.

Theme: Stallings William Network security essential

Date: / / □Sat □Sun □Mon □Tue □wed □Thu □Fri

(2016-2017)

Section 1.7 attack surface

→ Human attack surface

→ Software " "

→ Network " "

Attack Tree (Page 33)

→ Brutal account compromise

→ Brutal API insecure without access APIKey

→ SQL injection input not filter on sanitize or validition

→ ...mission ...user

Theme: Date: / /

X.800

Security Attack
Security mechanism
Security service

open design

Authenticity
Accountability.

Separation of privilege

Least privilege

complete mediation

Theme:

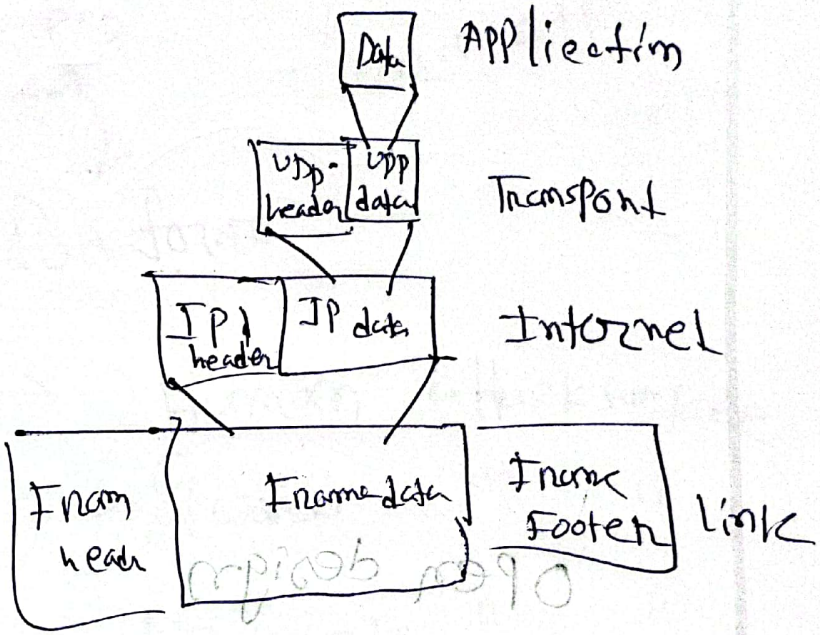
Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Book

Encapsulation

while design



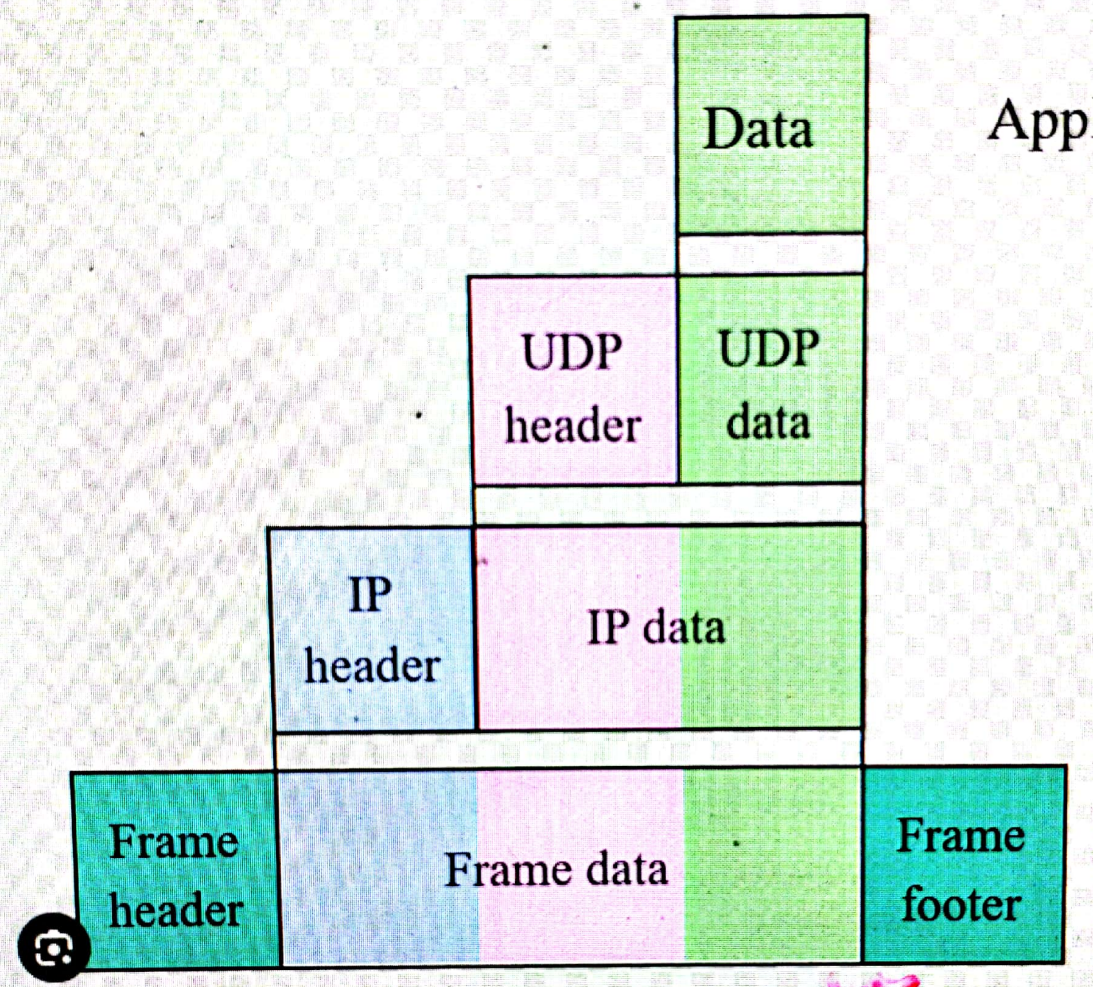
Modularity ⇒ আলাদা আলাদা

Layering ⇒ multifaction (2factor authentication)

Least astonishment ⇒

system যেভাবে চলবে বলে মনে হয় সেভাবে চলে

Wikipedia



Encapsulation (networking) - Wikipedia

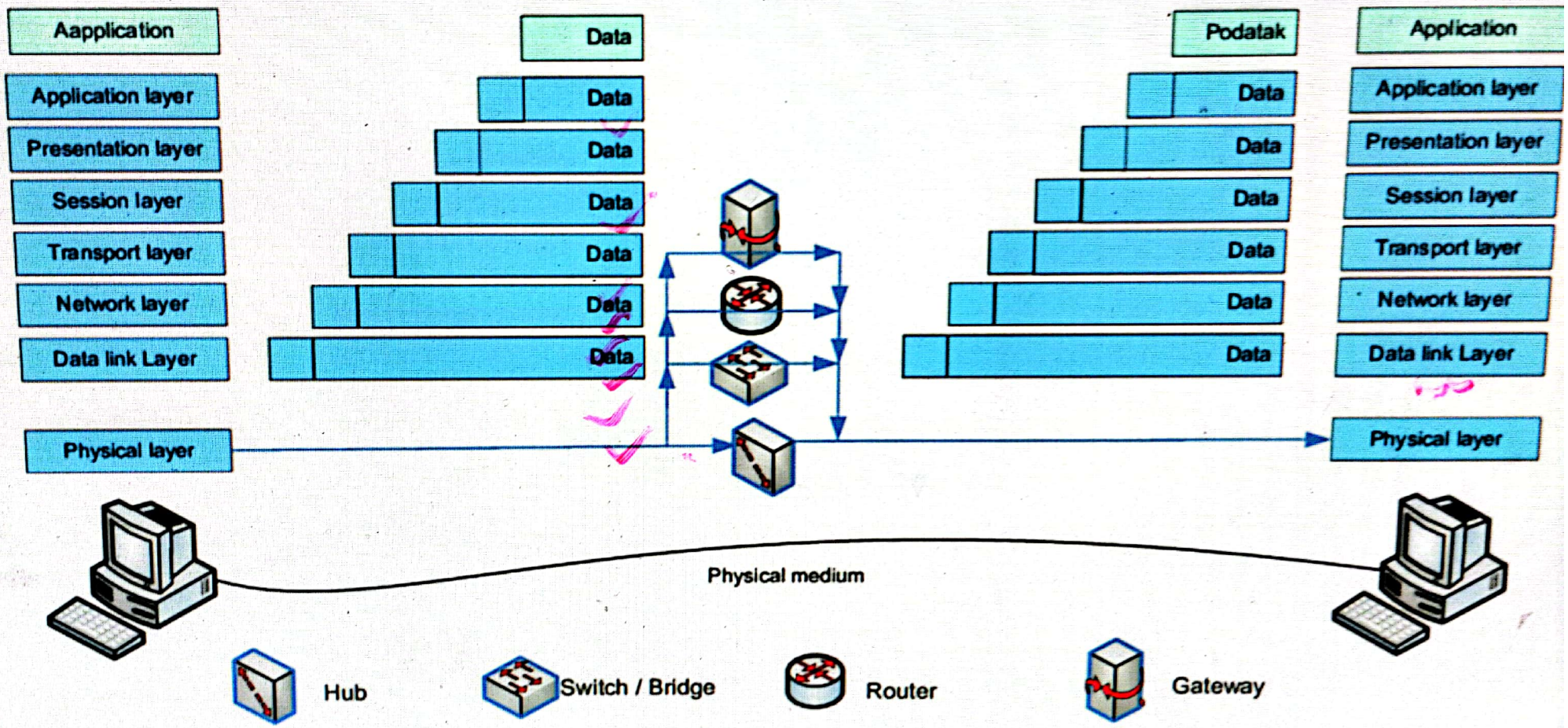
Visit

Images may be subject to copyright. Learn More

Share

Save

Security Payloa...



Theme:

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Diffie Hellman

এরা হচ্ছে

Symmetric Algorithm

Sentence vowel

যেগুলো use হয়

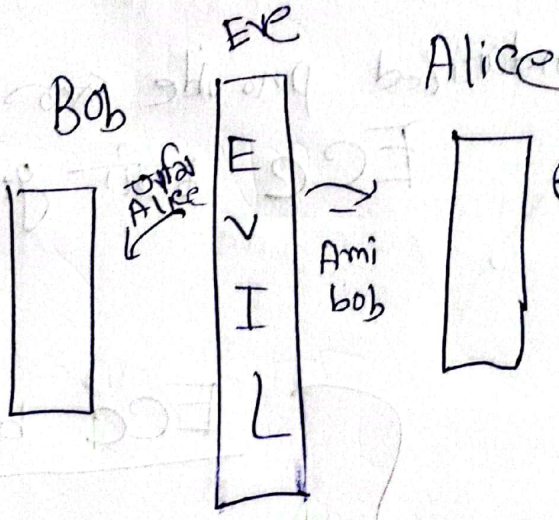
A, E, I, O, U,

এছাড়া আর vowel

আছে

semi vowel

W, Y, G, J



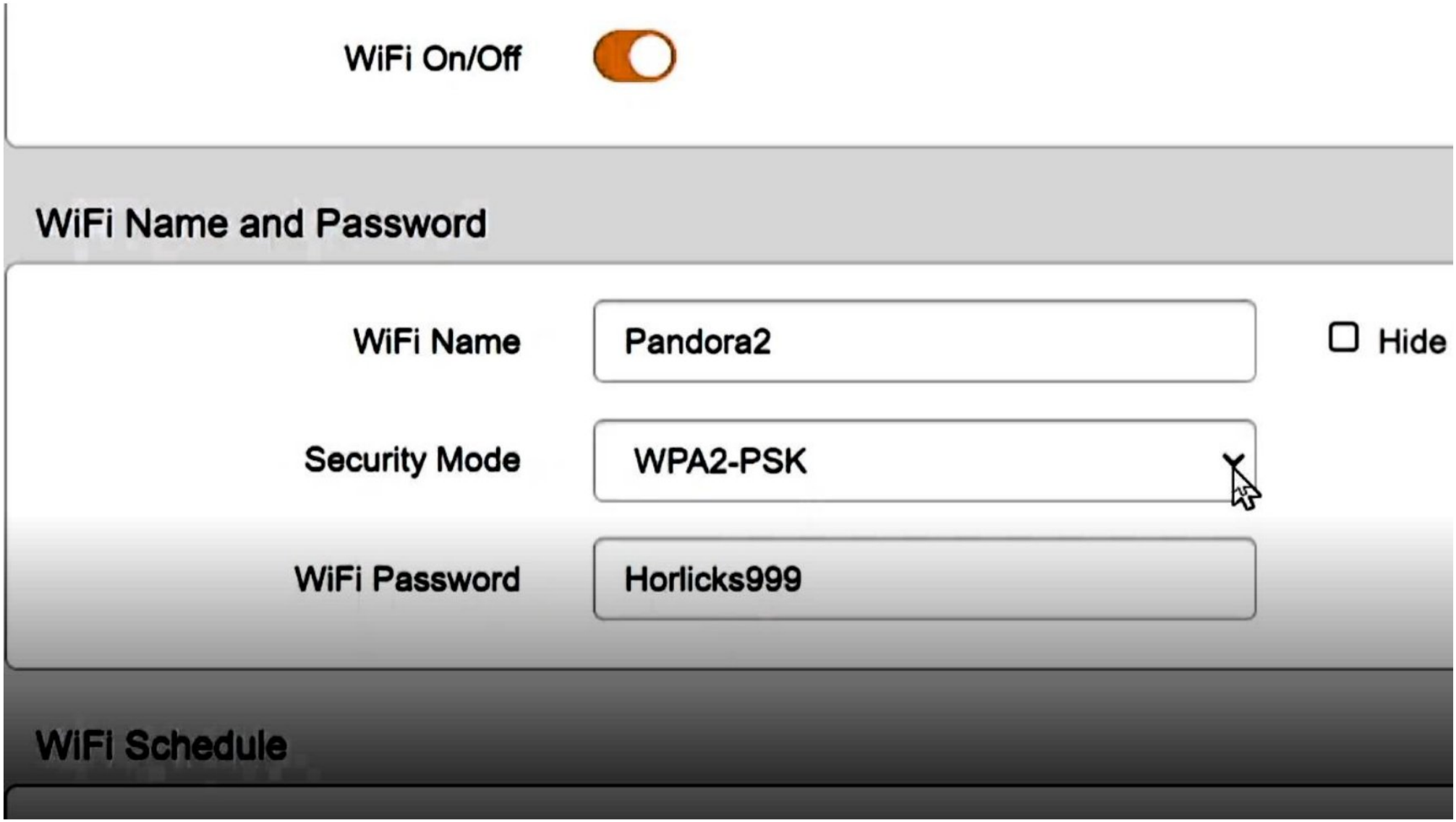
Man in the Middle Attack

Because of Notarization

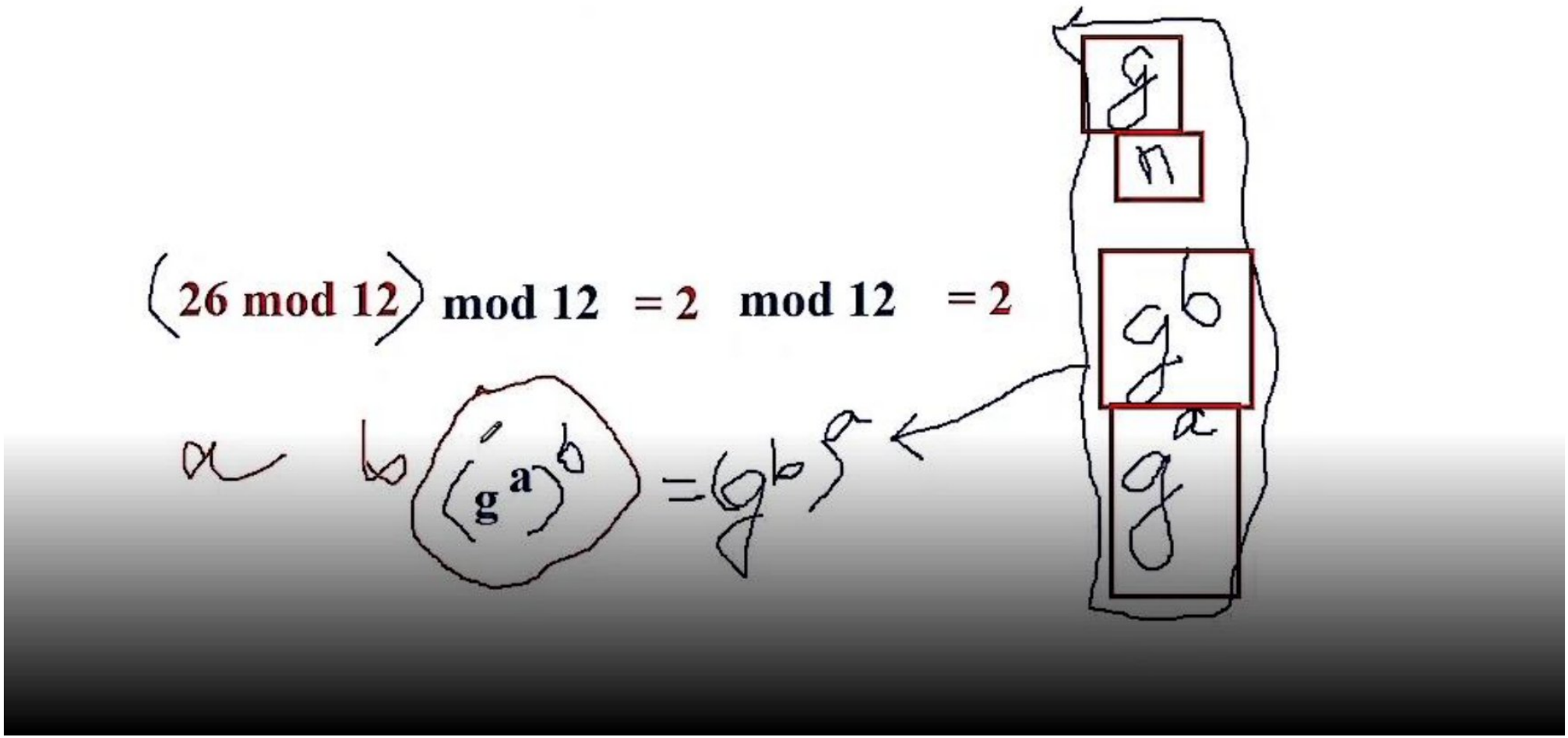
↓

অনুপস্থিত

Lack of Notarization.


WiFi On/Off
WiFi Name and Password
WiFi Name
Pandora2
Hide
Security Mode
WPA2-PSK
WiFi Password
Horlicks999
WiFi Schedule

$(26 \bmod 12) \bmod 12 = 2 \bmod 12 = 2$



g^a g^b

$$g^{ab} = g^{ba}$$

$$? = \frac{\log 4}{\log 2}$$

g^a g^b

$g^{ab} = g^{ba}$

Discrete Logarithm Problem (Hard Problem)

$? = \frac{\log 4}{\log 2}$

Discrete Logarithm Problem (Hard Problem)

Integer Factoring (Prime)

15 = 1, 3, 5

$15 = X = ?$ $= \{1, 3, \}$

Discrete Logarithm Problem (Hard Problem)

Integer Factoring (Prime)

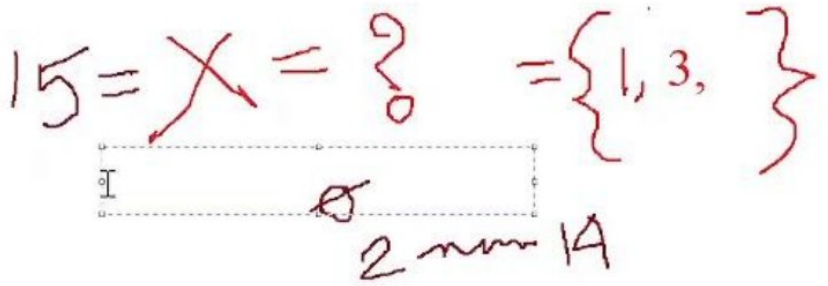
$15 = 1, 3, 5$

if x mod i $= 0$

Discrete Logarithm Problem (Hard Problem)

Integer Factoring (Prime)

15 = 1, 3, 5



if x mod i = 0

$15 = X = ? \quad = \{1, 3, \}$

$\sigma_{2 \text{ mm } 14}$

Discrete Logarithm Problem (Hard Problem)

Integer Factoring (Prime)

$15 = 1, 3, 5$

if x mod i = 0

one-way →

97

8091

83

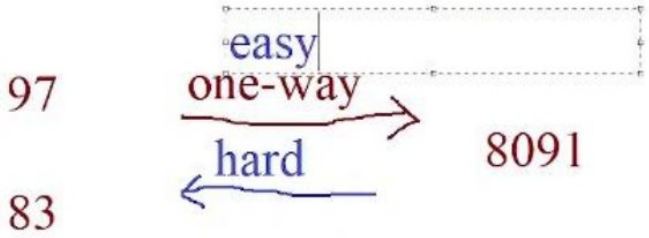
Discrete Logarithm Problem (Hard Problem)

Integer Factoring (Prime)

$15 = X = ?$ $= \{1, 3, \}$

$0 \leq 2 \leq 14$

$15 = 1, 3, 5$ if x mod (i) = 0



Discrete Logarithm Problem (Hard Problem)

$2 = g^{?} \bmod n$

$2 = 26 \bmod 12$

38
14
50
62
74

Integer Factoring (Prime)

Elliptic Curve Cr

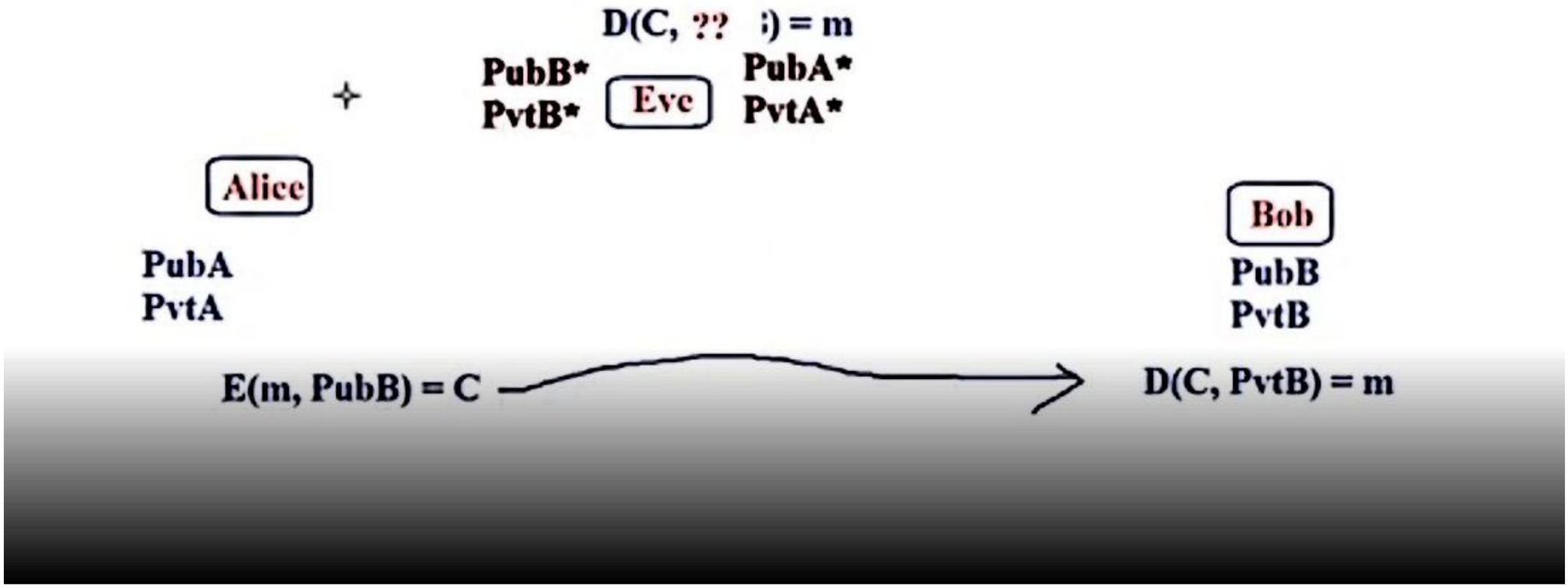
$15 = X = \{?\} = \{1, 3, \}$

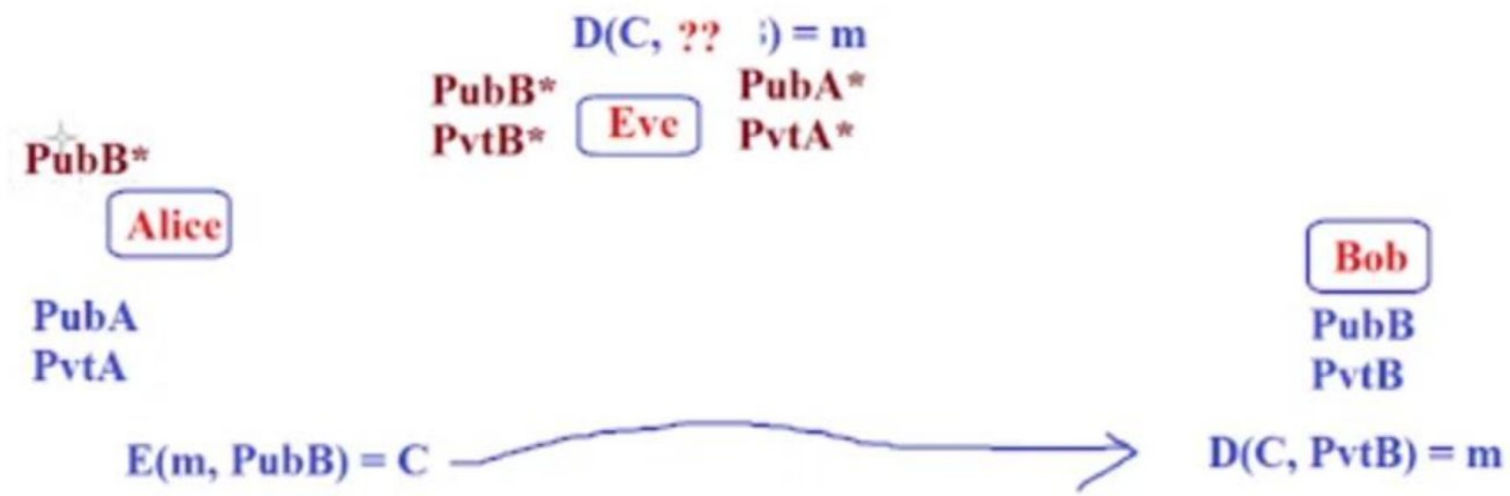
$\phi_{2 \text{ mm } 14}$

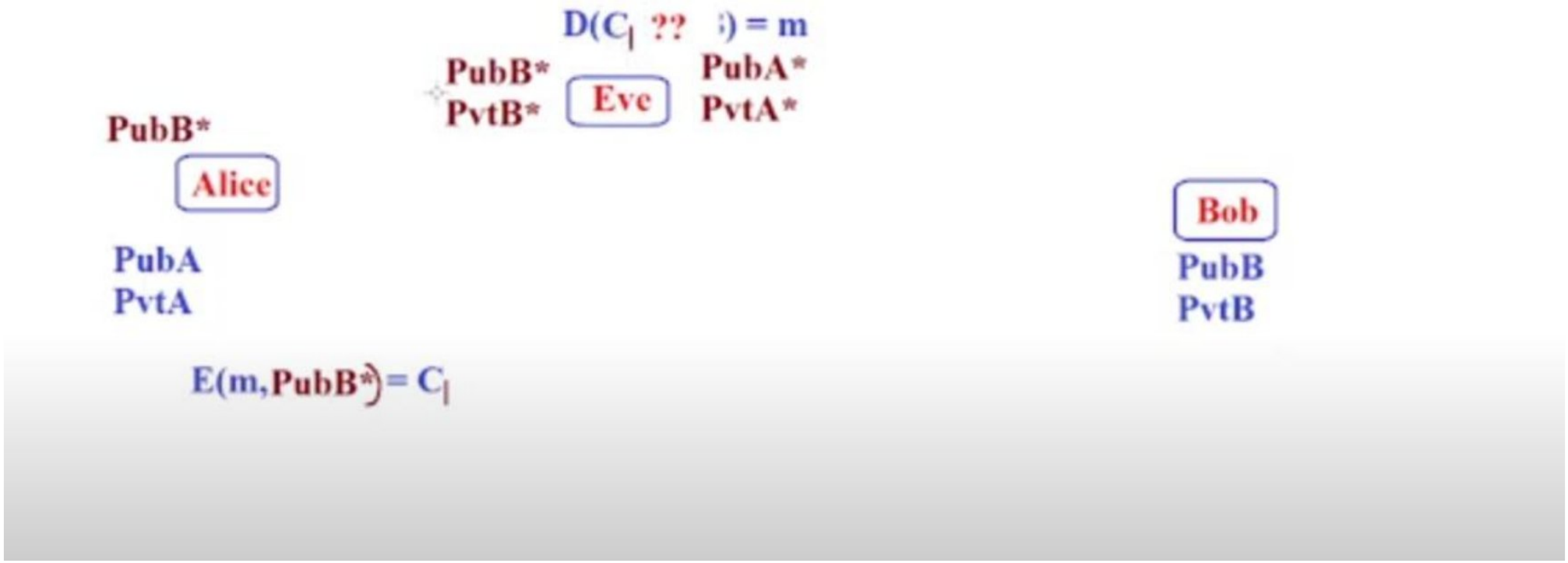
$15 = 1, 3, 5$

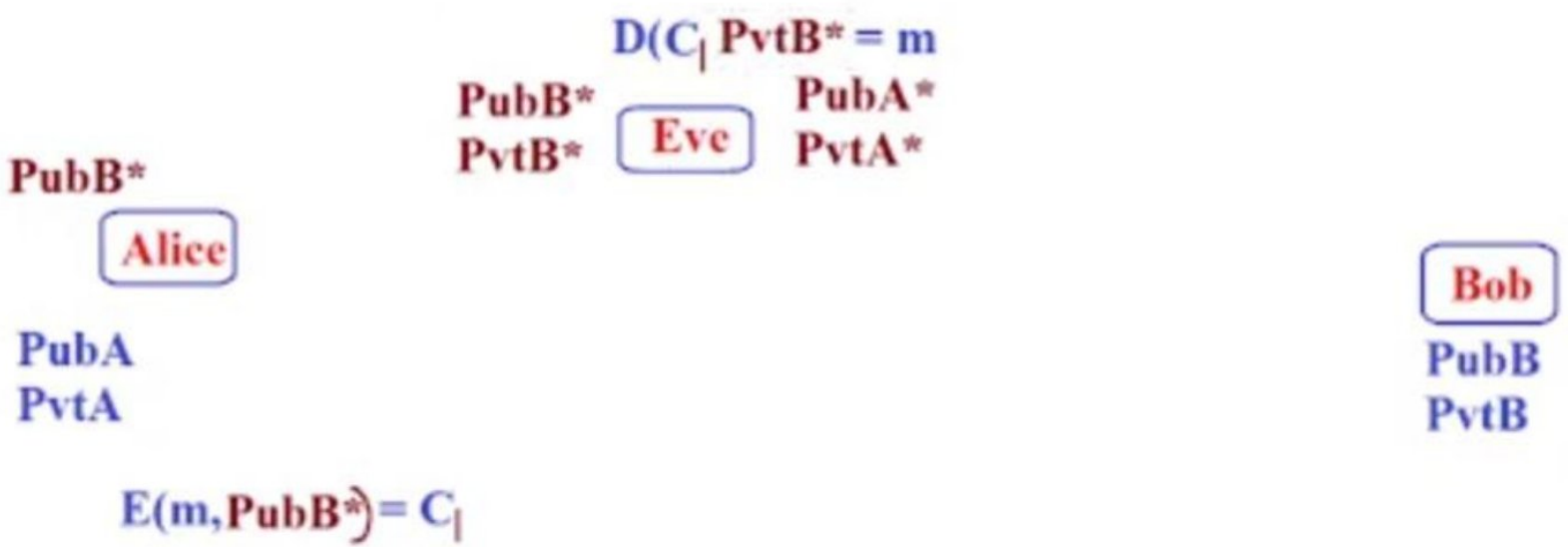
97 — easy one-way → 80

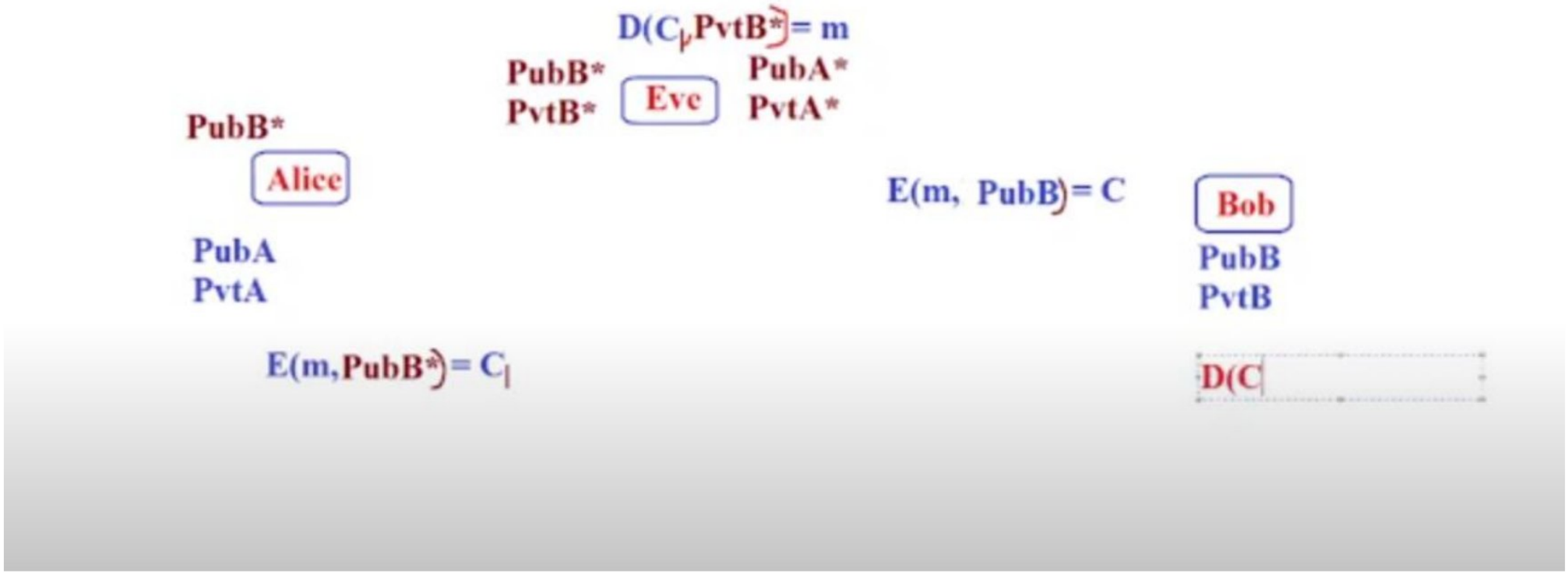
83 ← hard

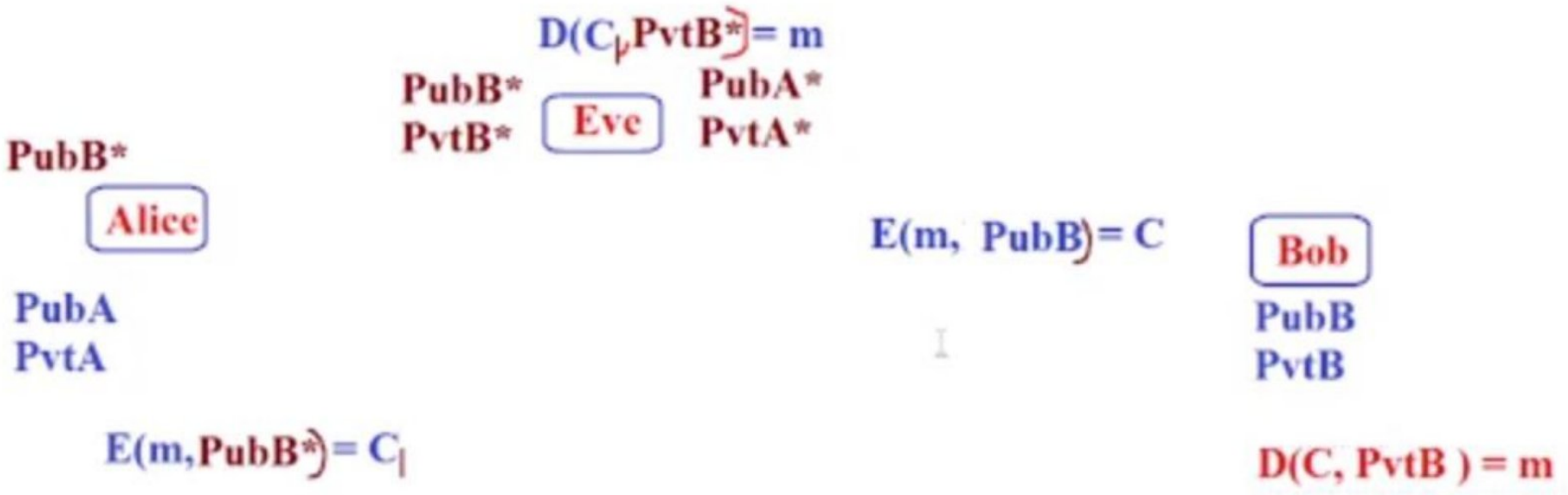

D(C, ?? ;) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
Alice
PubA
PvtA
Bob
PubB
PvtB
E(m, PubB) = C
D(C, PvtB) = m

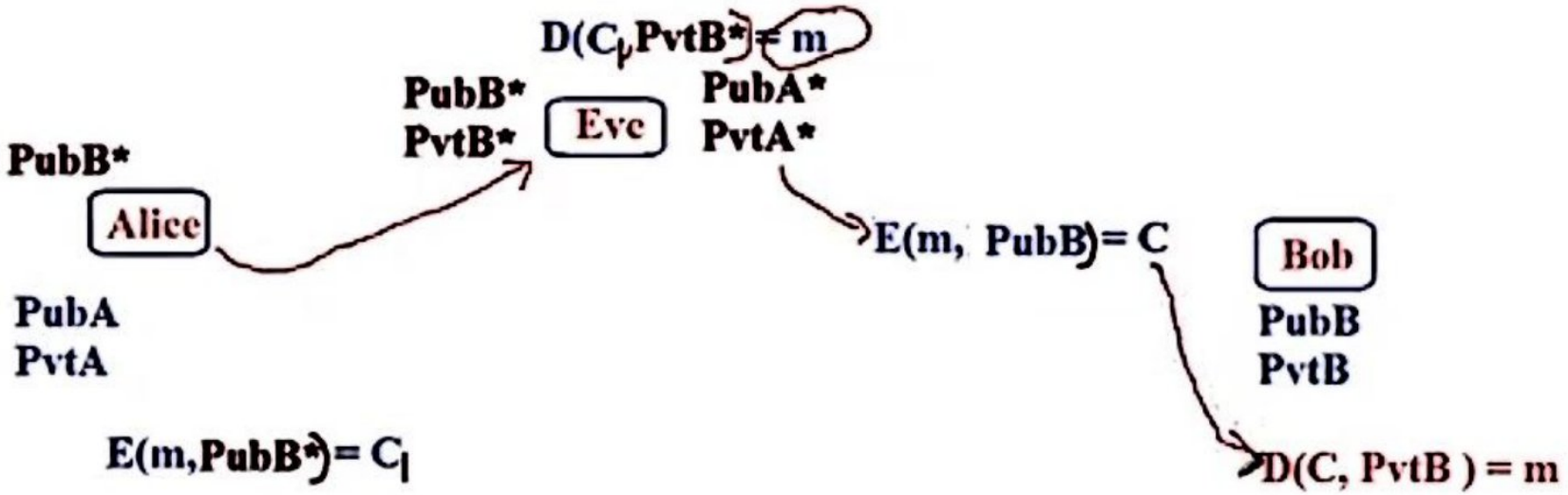

D(C, ??) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
PubA
PvtA
Bob
PubB
PvtB
E(m, PubB) = C
D(C, PvtB) = m

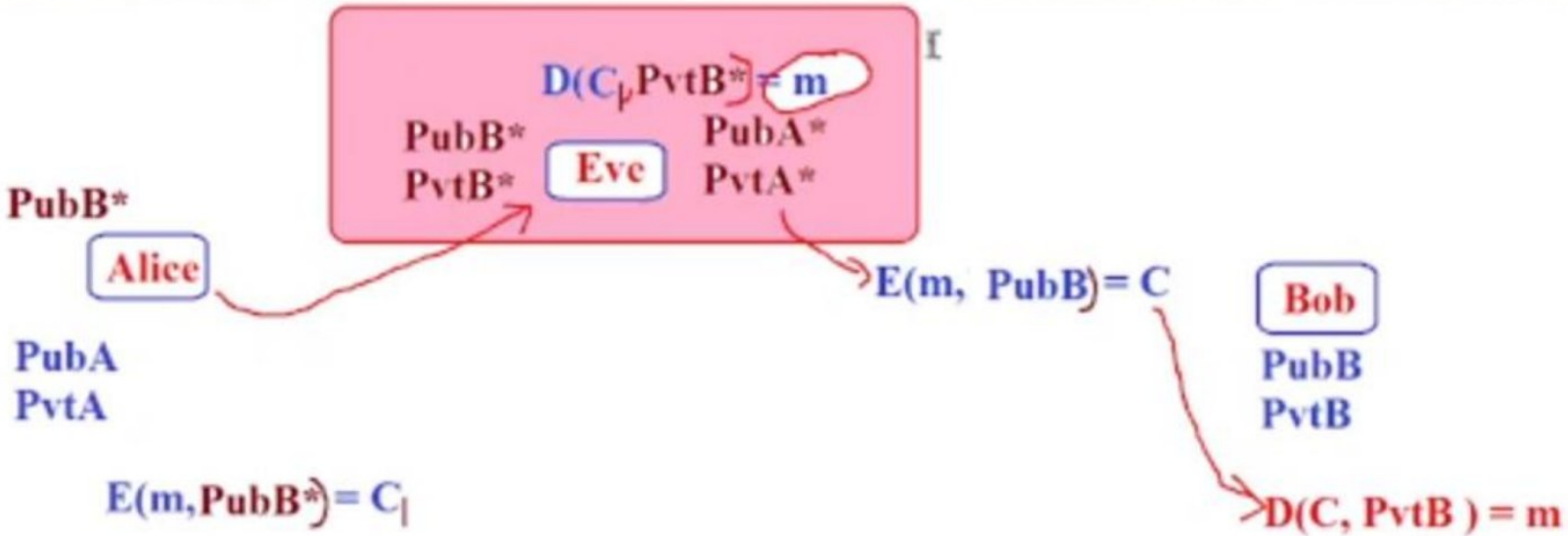

D(C| ?? ;) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
Bob
PubA
PvtA
PubB
PvtB
E(m,PubB*) = C|

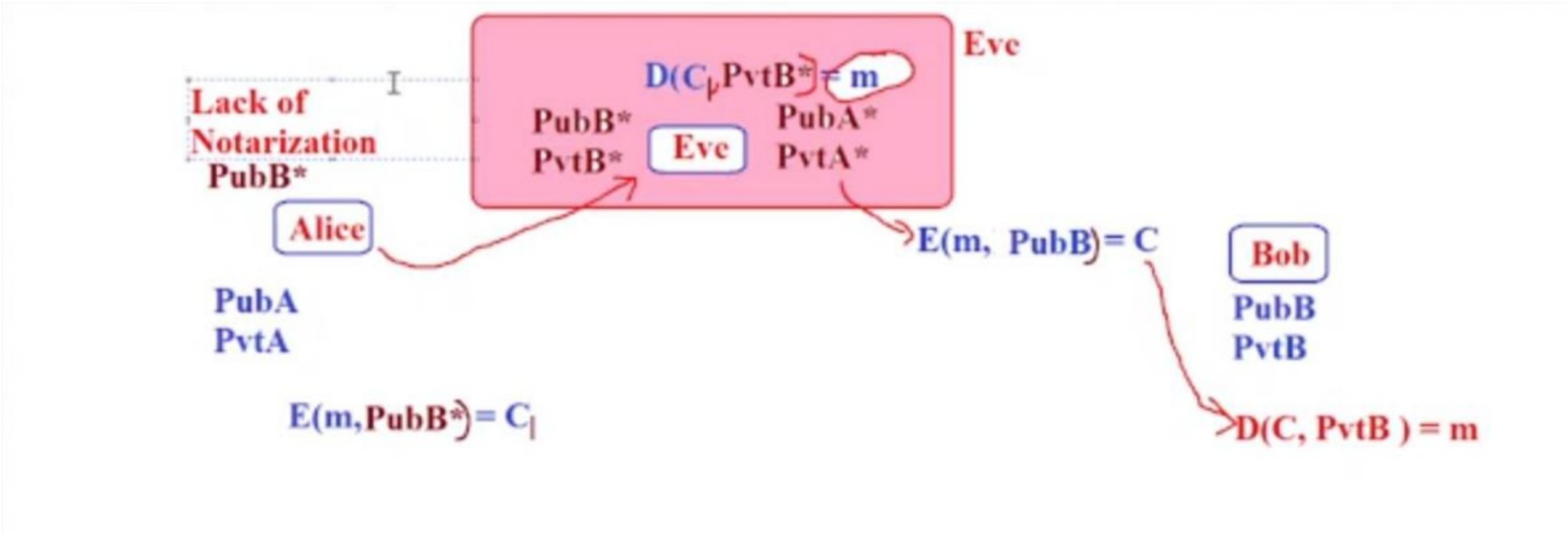

D(C, PvtB* = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
Bob
PubA
PvtA
PubB
PvtB
E(m,PubB*) = C,

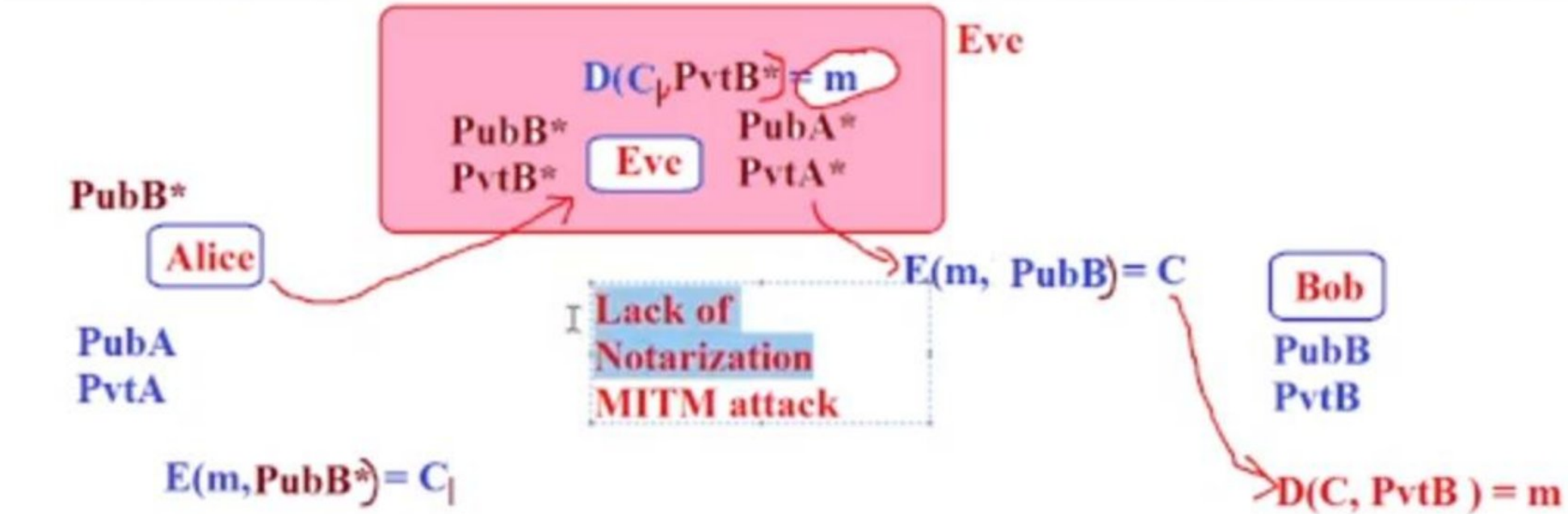

D(C, PvtB*) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
PubA
PvtA
E(m, PubB) = C
Bob
PubB
PvtB
E(m, PubB*) = C
D(C


D(C, PvtB*) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
E(m, PubB) = C
Bob
PubA
PvtA
PubB
PvtB
E(m, PubB*) = C
D(C, PvtB) = m

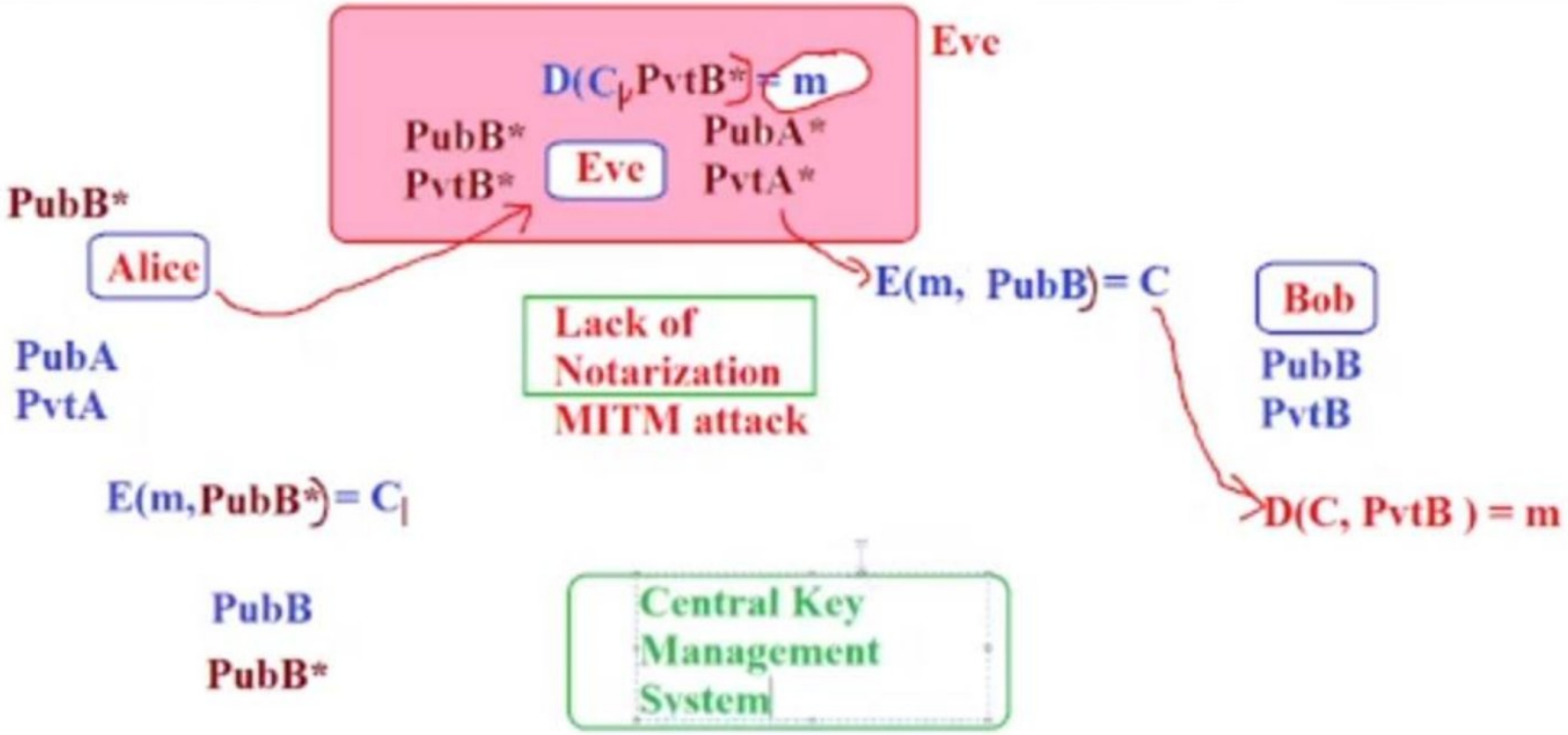

D(C, PvtB*) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
E(m, PubB) = C
Bob
PubA
PvtA
PubB
PvtB
E(m,PubB*) = C
D(C, PvtB) = m

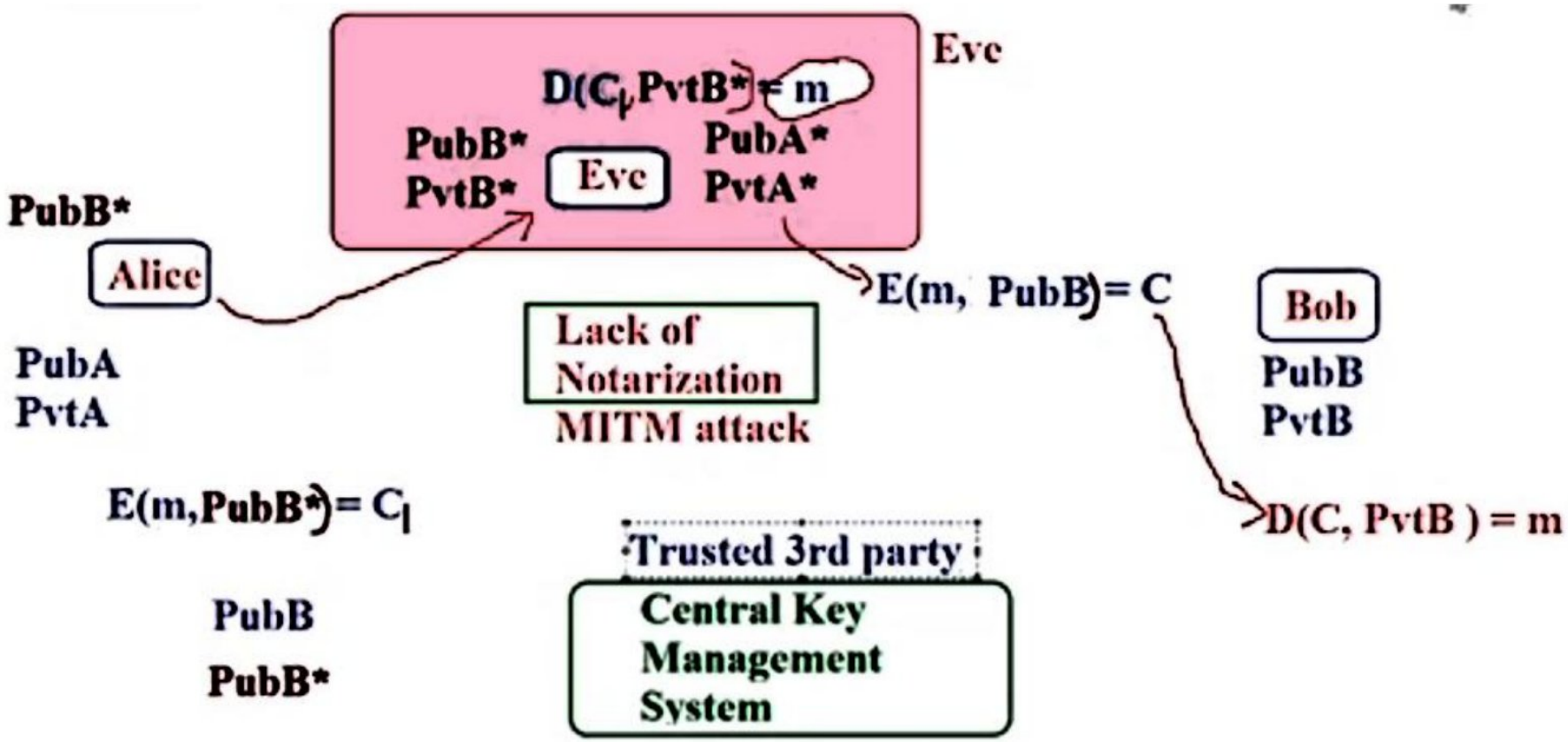

D(C, PvtB*) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
PubA
PvtA
E(m, PubB) = C
Bob
PubB
PvtB
E(m,PubB*) = C
D(C, PvtB) = m

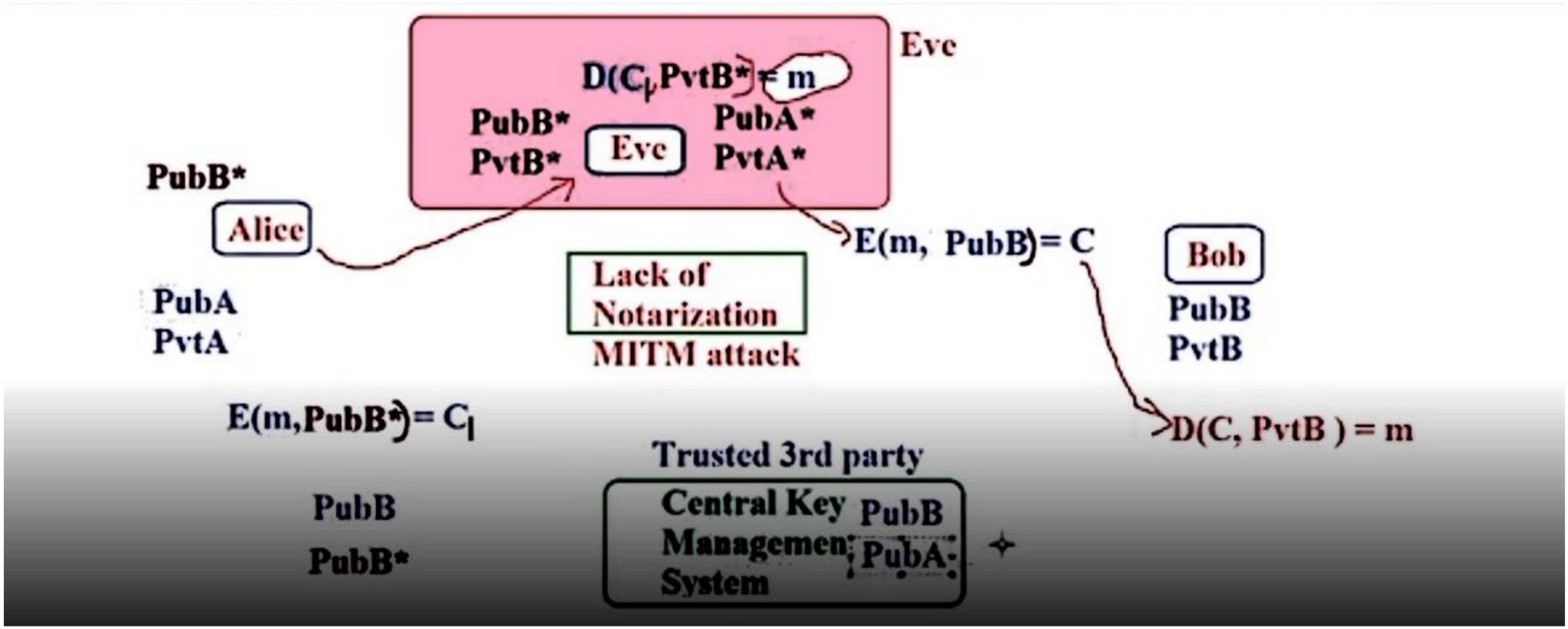

Eve
D(C, PvtB*) = m
Lack of
Notarization
PubB*
PubB*
PvtB*
Eve
PubA*
PvtA*
Alice
E(m, PubB) = C
Bob
PubA
PvtA
PubB
PvtB
E(m,PubB*) = C
D(C, PvtB) = m


Eve
D(C, PvtB*) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
PubA
PvtA
E(m, PubB) = C
Lack of
Notarization
MITM attack
Bob
PubB
PvtB
E(m,PubB*) = C
D(C, PvtB) = m

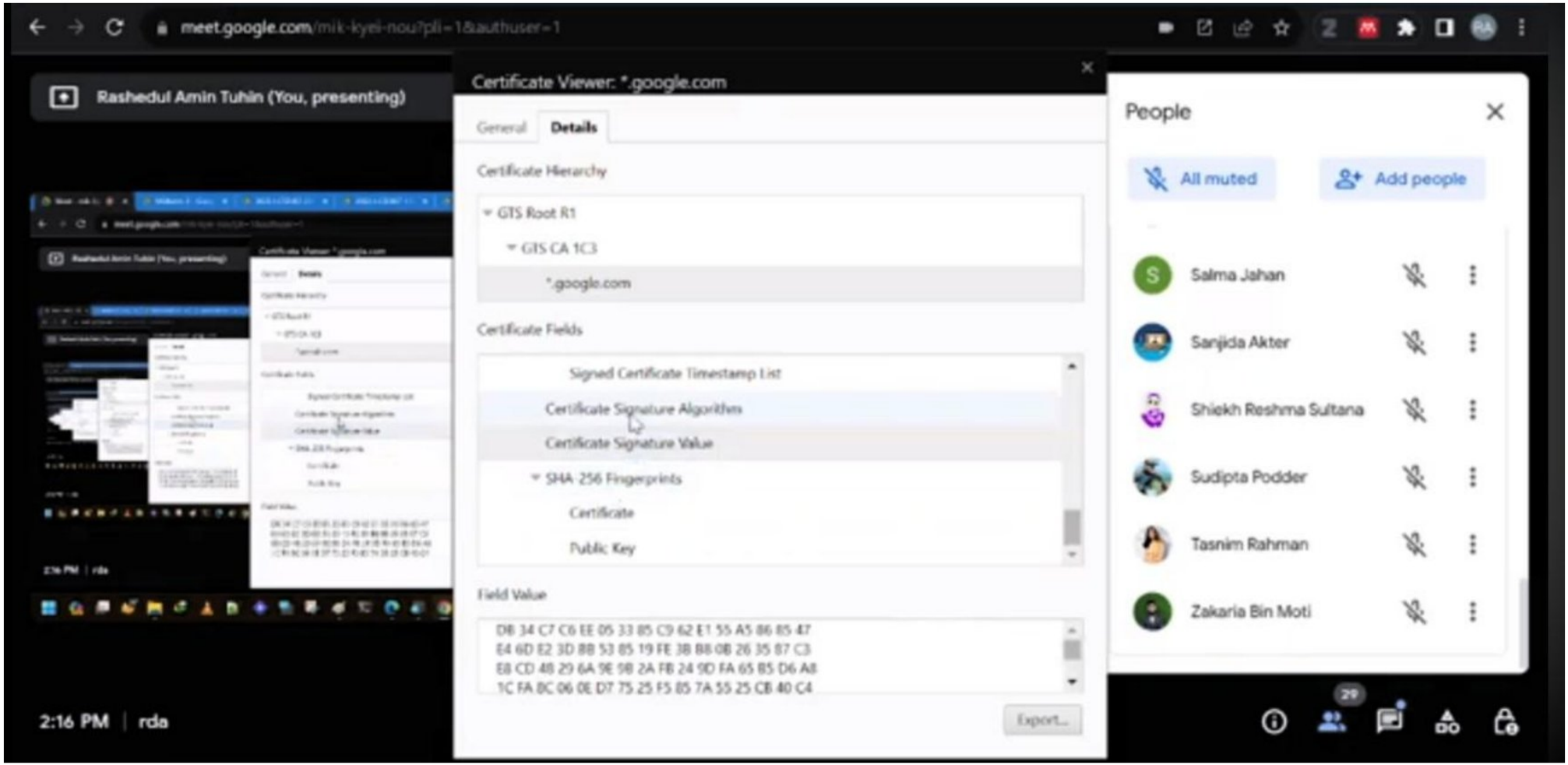

Eve
D(C, PvtB*) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
E(m, PubB) = C
Bob
PubB
PvtB
PubA
PvtA
Lack of
Notarization
MITM attack
D(C, PvtB) = m
E(m,PubB*) = C
Certification
Authority (CA
PubB
PubB*


Eve
D(C, PvtB*) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
E(m, PubB) = C
Bob
PubB
PvtB
Lack of
Notarization
MITM attack
PubA
PvtA
E(m, PubB*) = C
D(C, PvtB) = m
PubB
PubB*
Central Key
Management
System

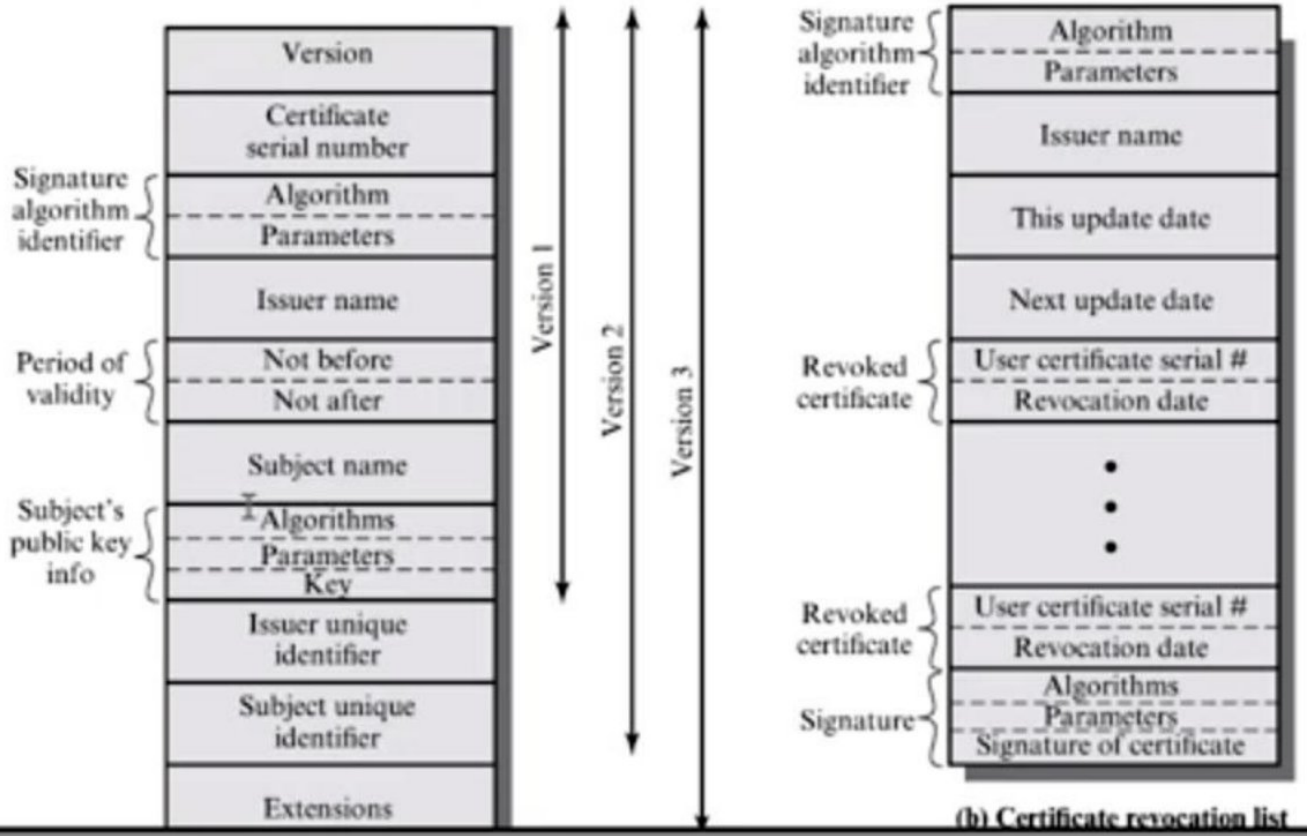

Eve
D(C, PvtB*) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
E(m, PubB) = C
Bob
PubB
PvtB
PubA
PvtA
Lack of
Notarization
MITM attack
D(C, PvtB) = m
E(m,PubB*) = C
Trusted 3rd party
PubB
PubB*
Central Key
Management
System


Eve
D(C, PvtB*) = m
PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
E(m, PubB) = C
Bob
Lack of
Notarization
MITM attack
PubA
PvtA
PubB
PvtB
E(m,PubB*) = C
D(C, PvtB) = m
Trusted 3rd party
PubB
PubB*
Central Key
Managemen
System
PubB
PubA

X.509 Certificates

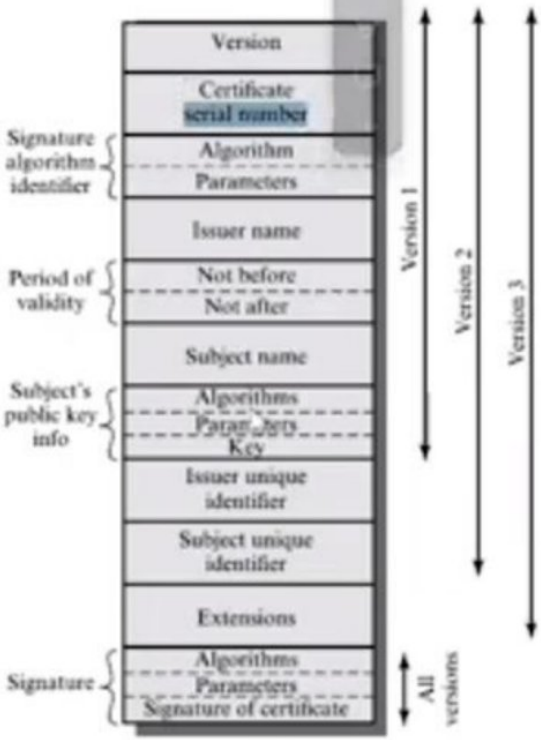

meet.google.com/mik-kyei-nou?pli=1&authuser=1
Rashedul Amin Tuhin (You, presenting)
Certificate Viewer: *.google.com
General
Details
Certificate Hierarchy
GTS Root R1
GTS CA 1C3
*.google.com
Certificate Fields
Signed Certificate Timestamp List
Certificate Signature Algorithm
Certificate Signature Value
SHA-256 Fingerprints
Certificate
Public Key
Field Value
DB 34 C7 C6 EE 05 33 85 C9 62 E1 55 A5 86 85 47
E4 6D E2 3D 88 53 85 19 FE 38 B8 0B 26 35 87 C3
E8 CD 48 29 6A 9E 98 2A FB 24 9D FA 65 B5 D6 A8
1C FA BC 06 0E D7 75 25 F5 85 7A 55 25 CB 40 C4
Export...
People
All muted
Add people
Salma Jahan
Sanjida Akter
Shiekh Reshma Sultana
Sudipta Podder
Tasnim Rahman
Zakaria Bin Moti
2:16 PM | rda

identifier are present, the value must be version 2. If one or more extensions

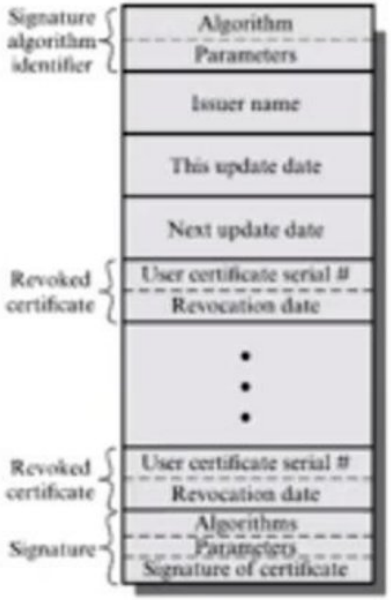


(b) Certificate revocation list

the default is version 1. If the Issuer Unique Identifier or Subject Unique Identifier are present, the value must be version 2. If one or more extensions

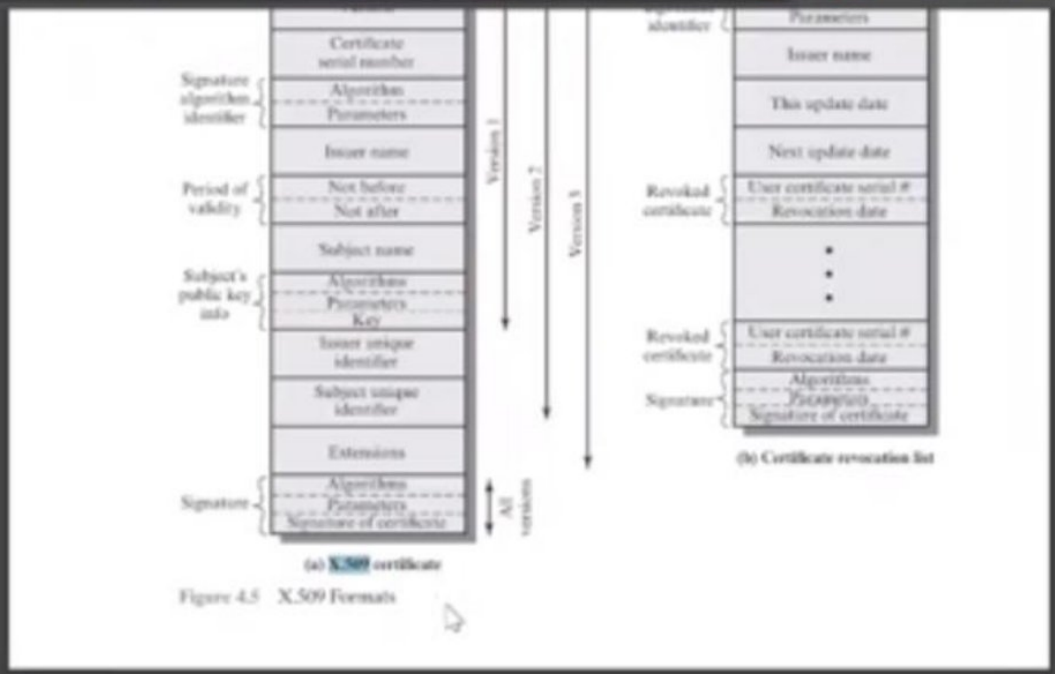


(a) X.509 certificate



(b) Certificate revocation list

Figure 4.5 X.509 Formats



(a) X.509 certificate

(b) Certificate revocation list

Figure 4.5 X.509 Formats

are present, the version must be version 3. Although the X.509 specification is currently at version 7, no changes have been made to the fields that make up the certificate since version 3.

- **Serial number:** An integer value, unique within the issuing CA, that is unambiguously associated with this certificate.

Text Tools Untitled - Paint

File Home View Text

Cut Copy Paste Clipboard

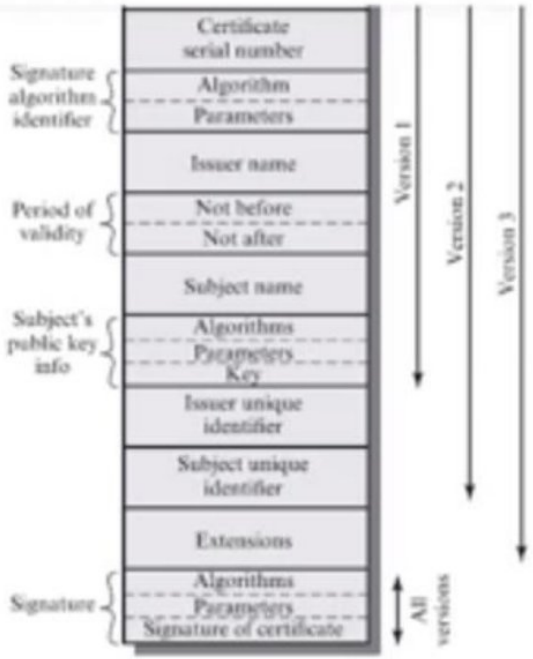
Times New Roman 20 B I U abc Font

Opaque Transparent Background

Color 1 Color 2 Edit colors Colors

X.509 Certificates

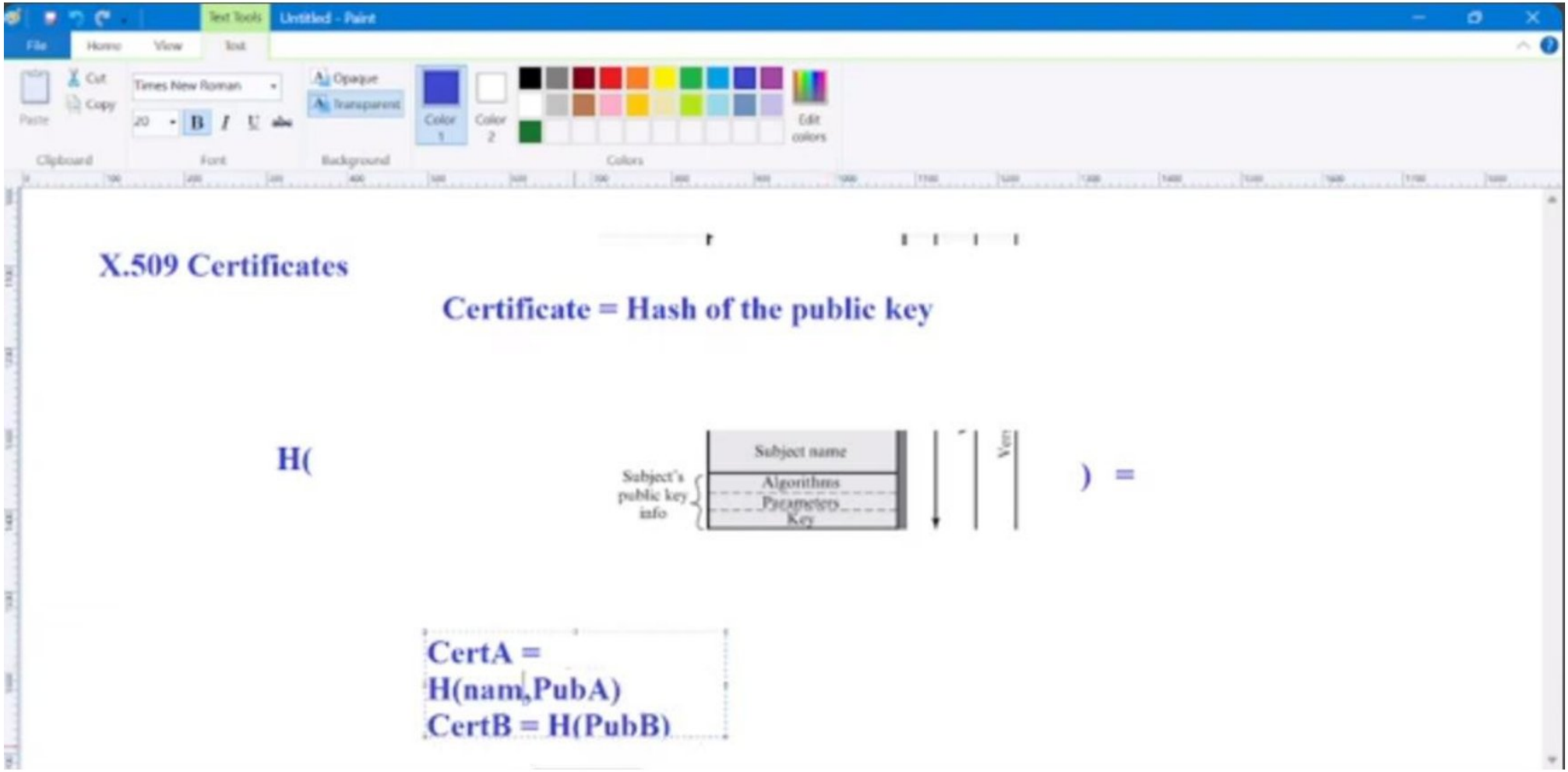
H(



) = 256

1 × 1px 7580 × 3392px 100%

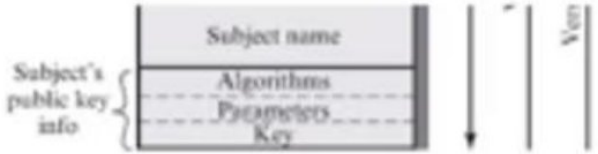
97.0 KB/s 4.70 KB/s ENG 14:19 2023-11-22


Text Tools
Untitled - Paint
File
Home
View
Text
Cut
Copy
Paste
Times New Roman
20
B
I
U
Opaque
Transparent
Color 1
Color 2
Edit colors
Clipboard
Font
Background
Colors
X.509 Certificates
Certificate = Hash of the public key
H(
Subject name
Subject's public key info
Algorithms
Parameters
Key
Ver
) =
CertA = H(nam,PubA)
CertB = H(PubB)

X.509 Certificates

Certificate = Hash of the public key

H(



) =

CertA = H(name, asdf, asdf ,asdf asdfasdfasdf l, asfasdfas,PubA)
CertB = H(PubB)

09 Certificates

Certificate = Hash of the public key

CertA = H(PubA)
CertB = H(PubB)

H(

) =

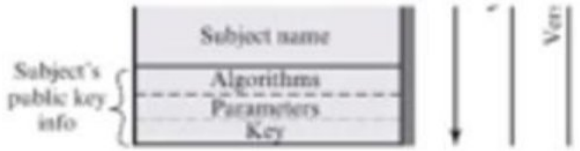
Signing = to encrypt with the private key

09 Certificates

Certificate = Hash of the public key

CertA = H(PubA)
CertB = H(PubB)

H(



) =

Signing = to encrypt with the private key

SignedCertA = E (CertA, PvtA)

ublic key

CertA = H(PubA)
CertB = H(PubB)

CA

P

) =

vate key

SignedCertA = E (CertA, PvtA)

ublic key

CertA = H(PubA)
CertB = H(PubB)

CA

PubCA
PvtCA

) =

vate key

SignedCertA = E (CertA, PvtA)

ublic key

CertA = H(PubA)
CertB = H(PubB)

CA

PubCA
PvtCA

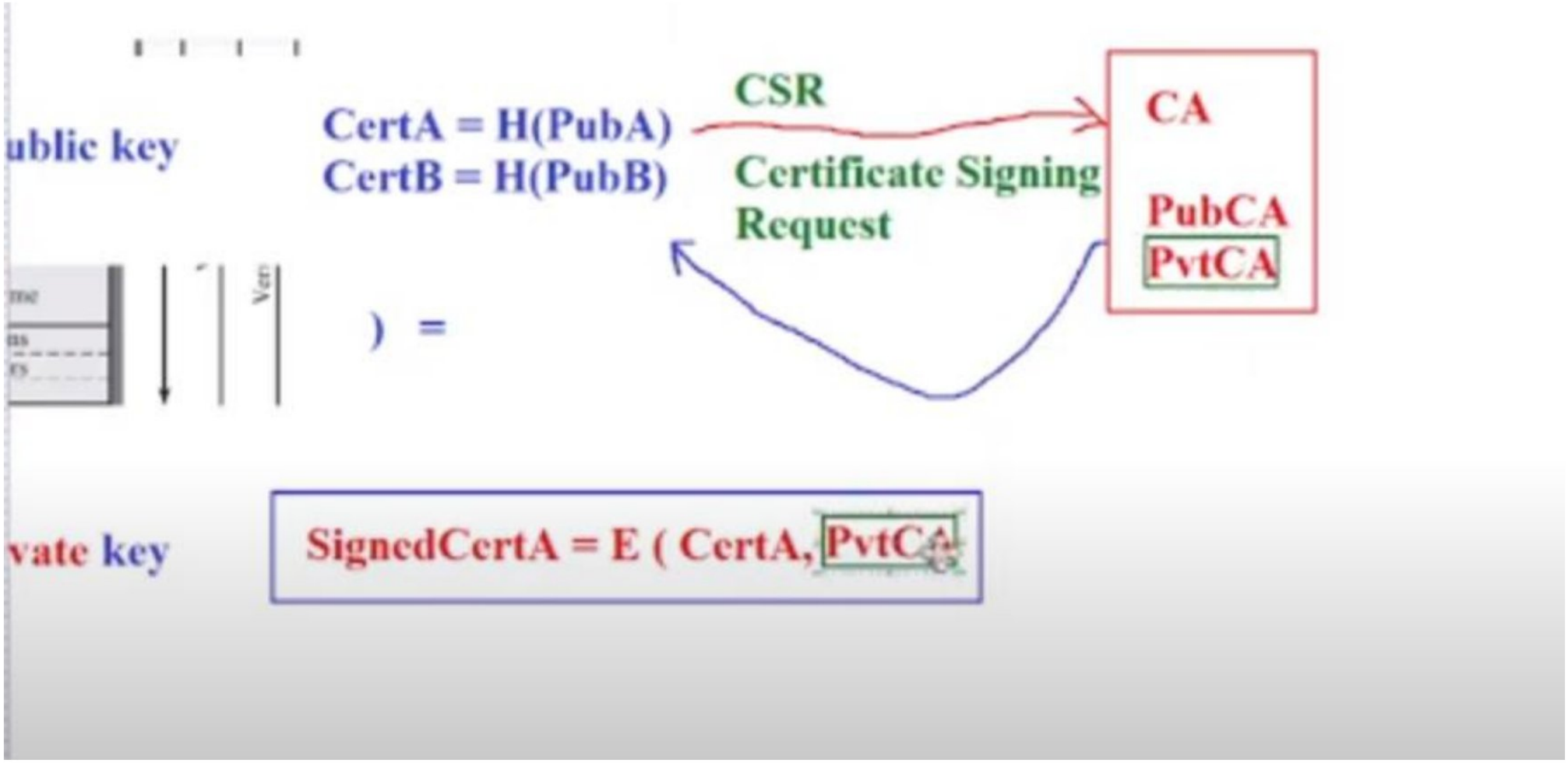
) =

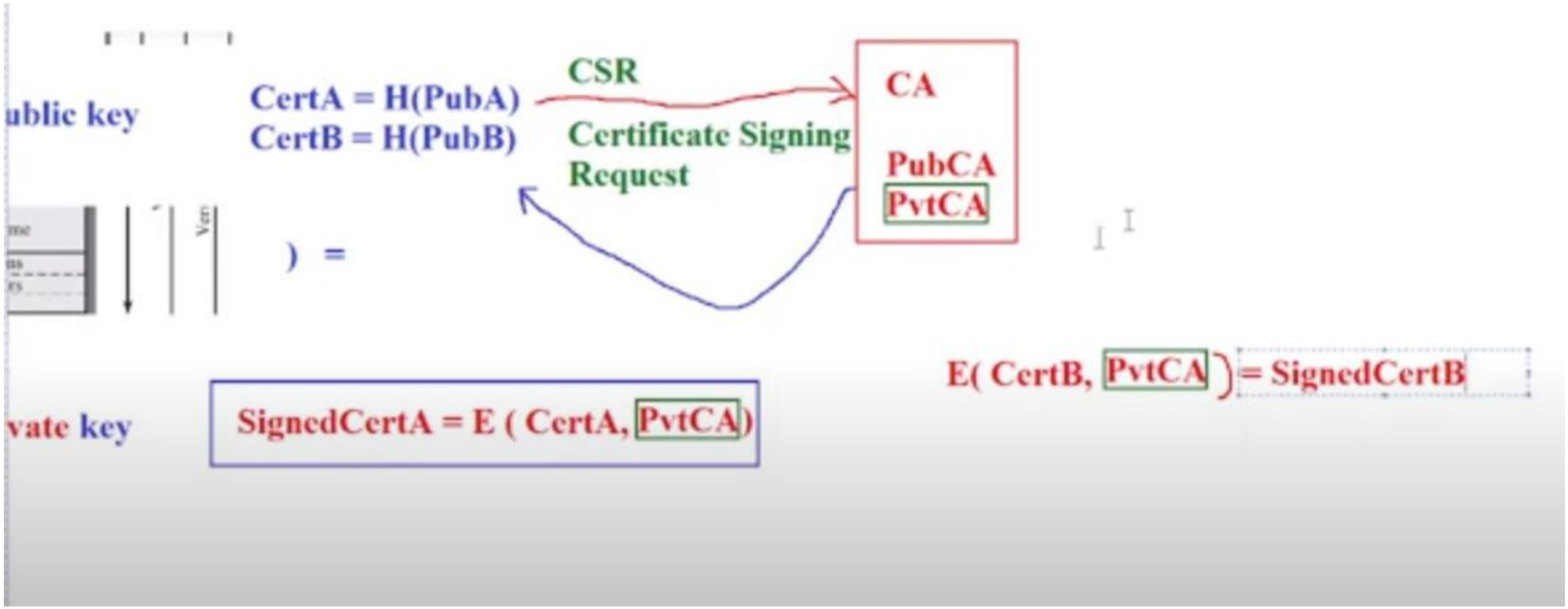
vate key

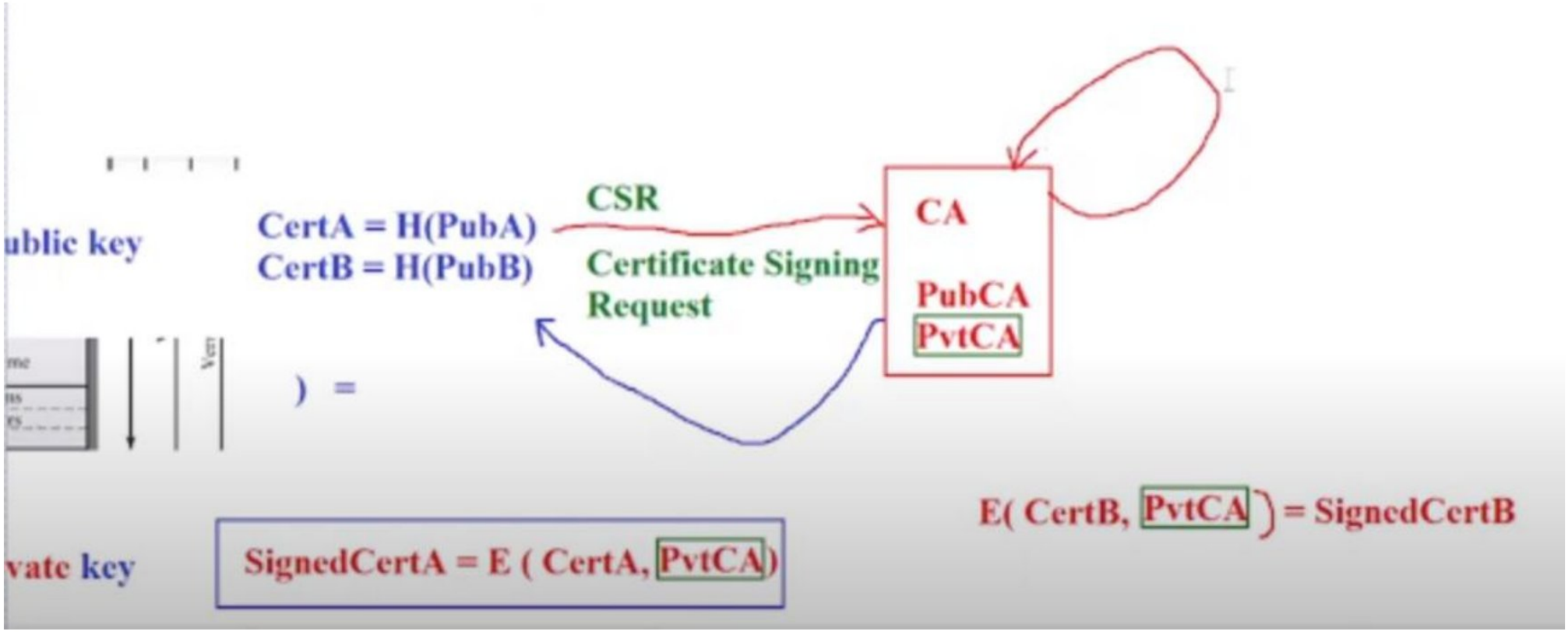
SignedCertA = E (CertA, PvtA)

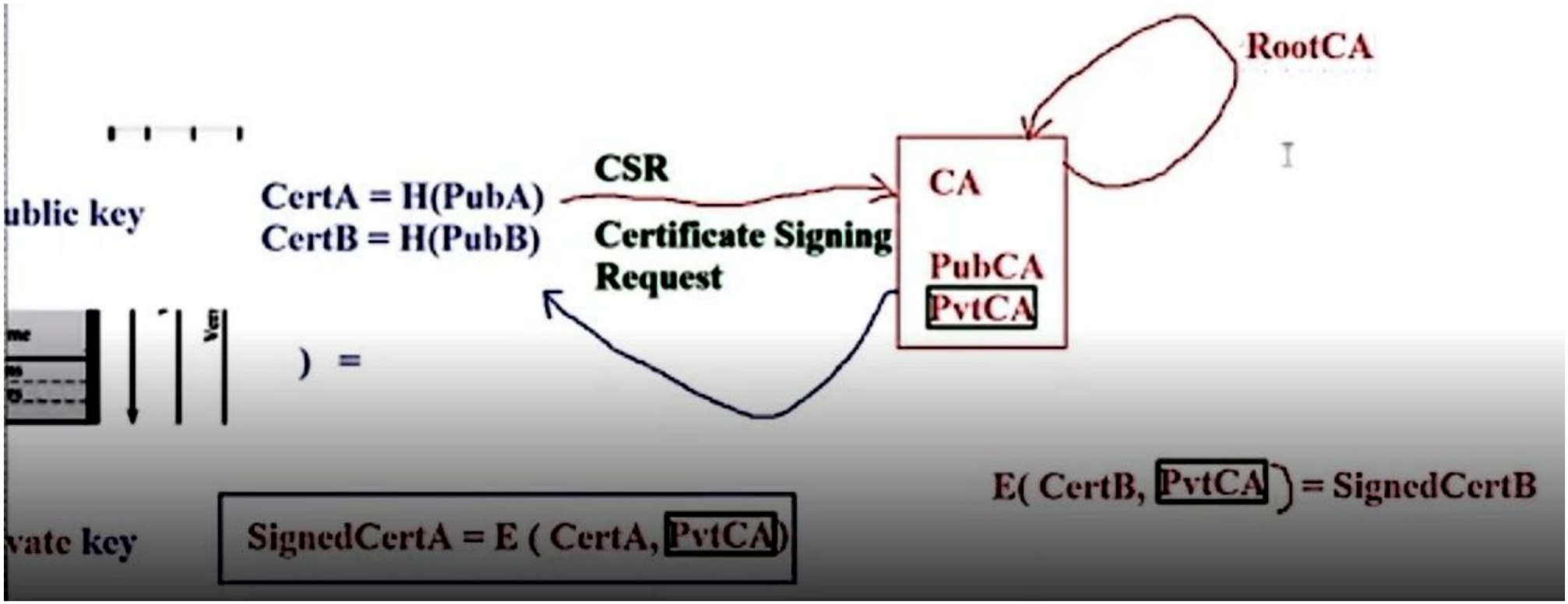

ublic key
CertA = H(PubA)
CertB = H(PubB)
CSR
Certificate Signing
Request
CA
PubCA
PvtCA
) =
vate key
SignedCertA = E (CertA, PvtA)

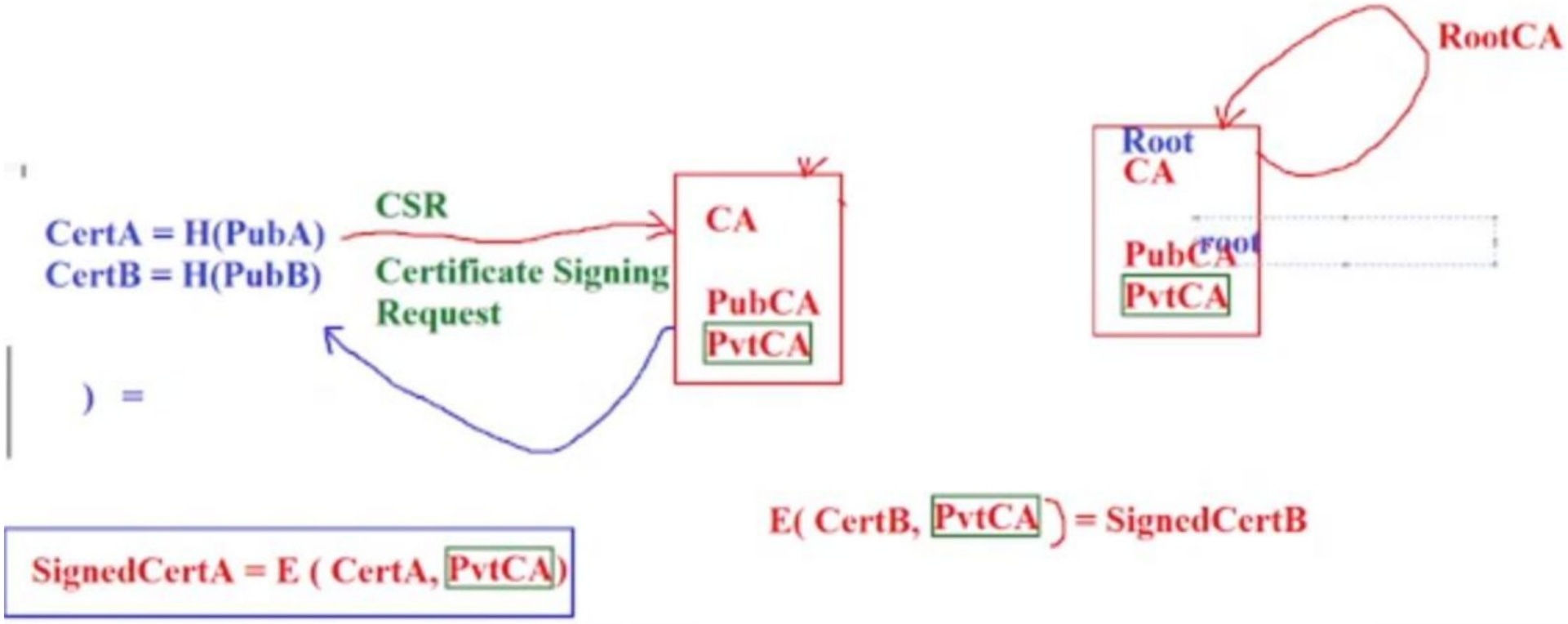

ublic key
CertA = H(PubA)
CertB = H(PubB)
CSR
Certificate Signing Request
CA
PubCA
PvtCA
) =
vate key
SignedCertA = E (CertA,)

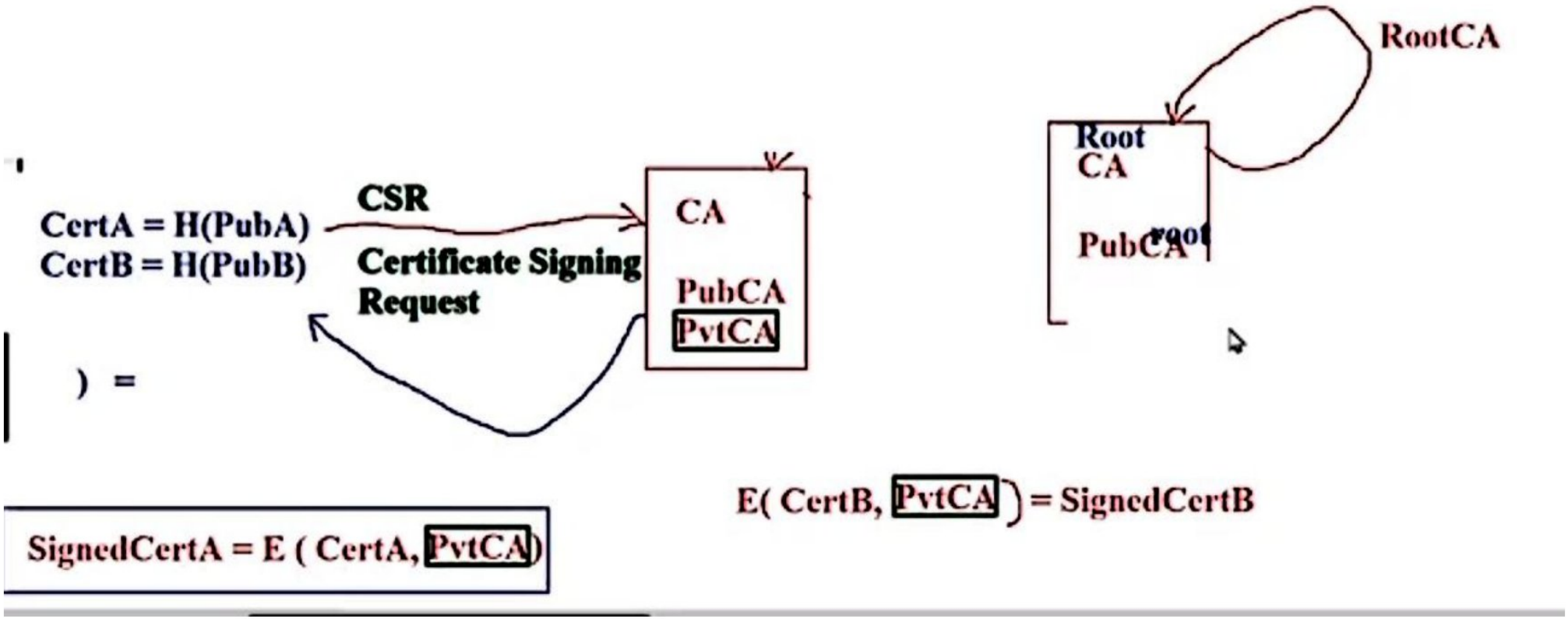

ublic key
CertA = H(PubA)
CertB = H(PubB)
CSR
Certificate Signing Request
CA
PubCA
PvtCA
) =
vate key
SignedCertA = E (CertA, PvtCA


ublic key
CertA = H(PubA)
CertB = H(PubB)
CSR
Certificate Signing Request
CA
PubCA
PvtCA
) =
vate key
SignedCertA = E (CertA, PvtCA)
E(CertB, PvtCA) = SignedCertB

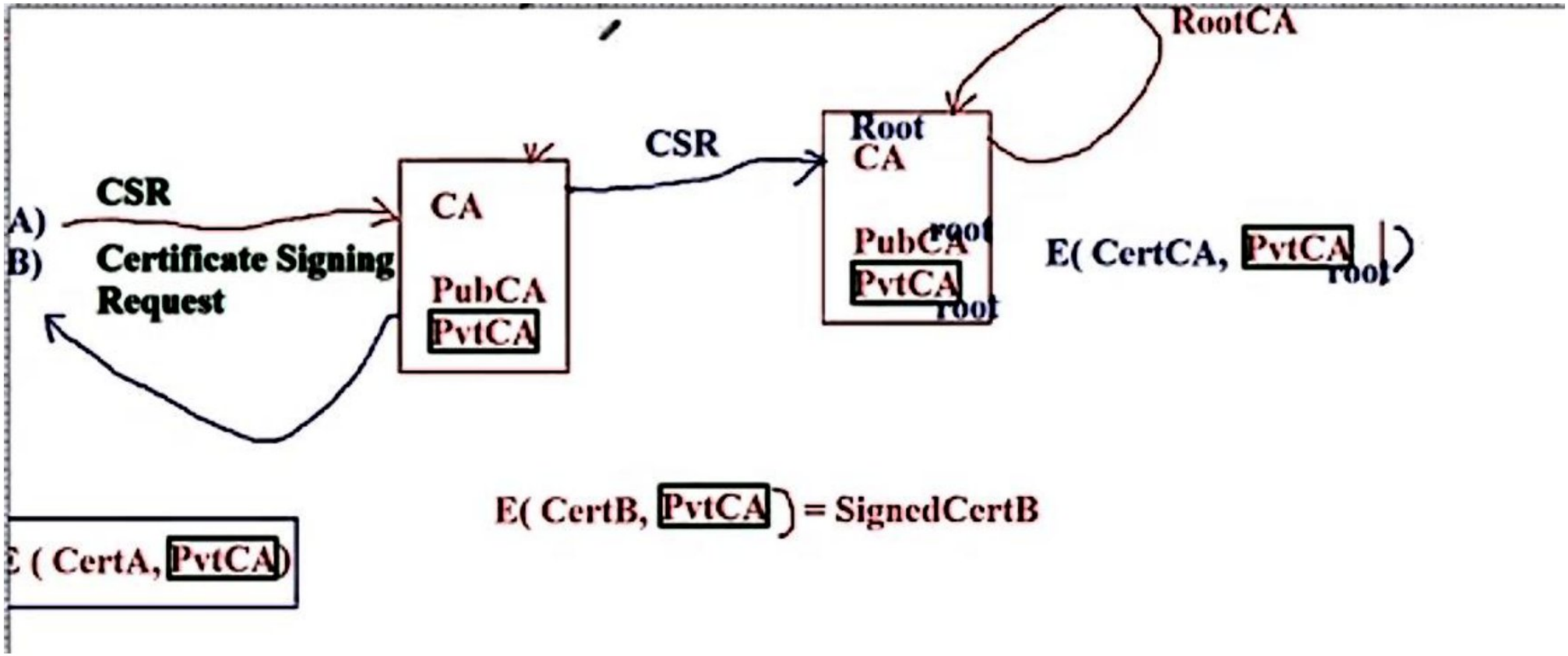

ublic key
CertA = H(PubA)
CertB = H(PubB)
CSR
Certificate Signing Request
CA
PubCA
PvtCA
) =
vate key
SignedCertA = E (CertA, PvtCA)
E(CertB, PvtCA) = SignedCertB

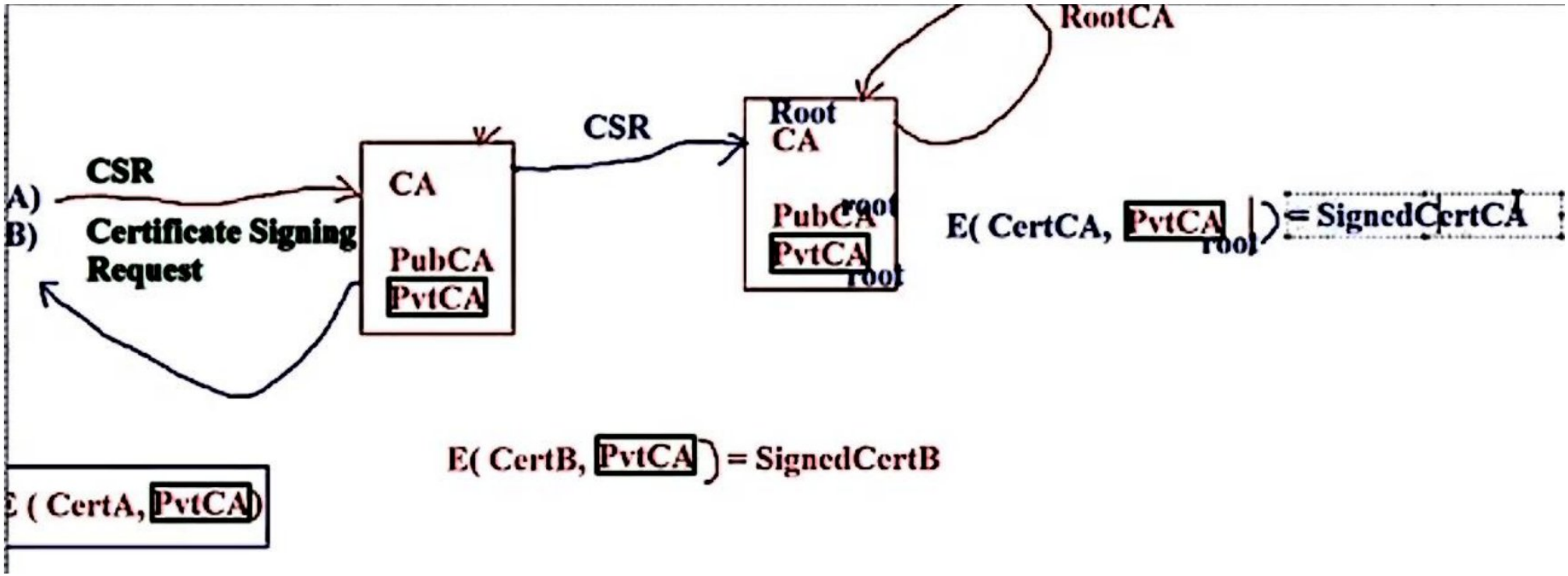

RootCA
ublic key
CertA = H(PubA)
CertB = H(PubB)
CSR
Certificate Signing Request
CA
PubCA
PvtCA
) =
E(CertB, PvtCA) = SignedCertB
vate key
SignedCertA = E (CertA, PvtCA)

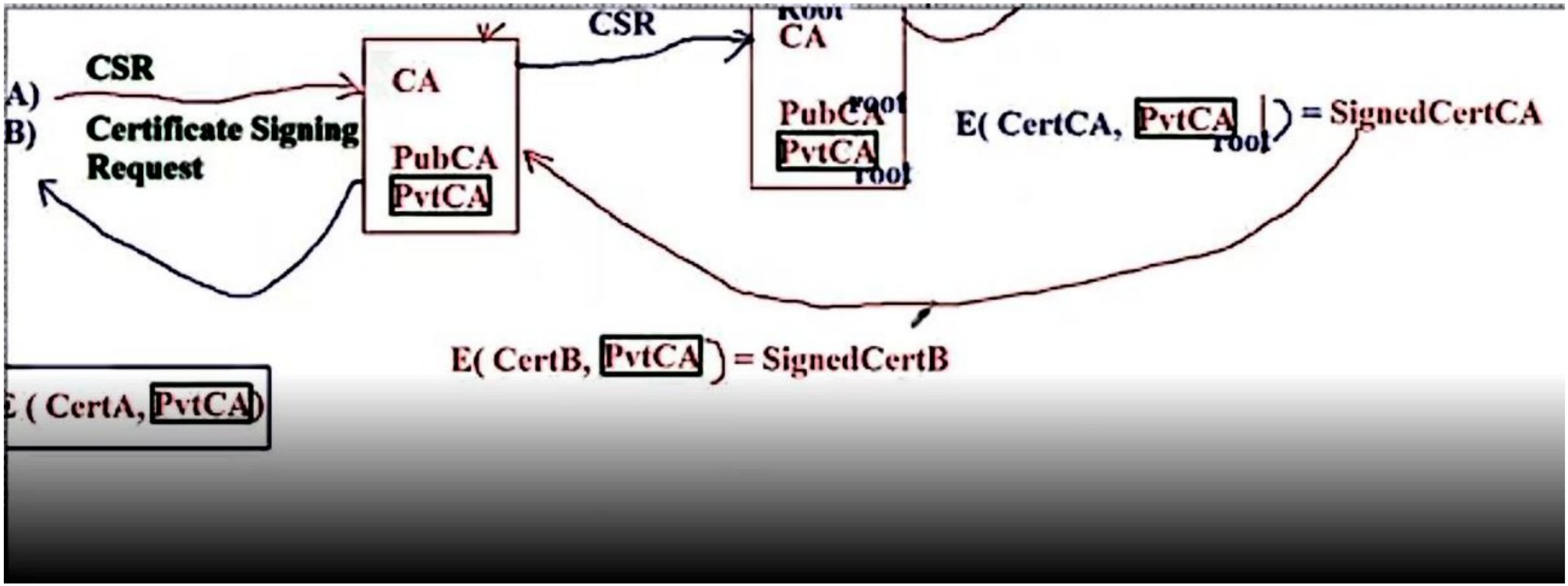

RootCA
Root
CA
PubCA
PvtCA
CertA = H(PubA)
CertB = H(PubB)
CSR
Certificate Signing
Request
CA
PubCA
PvtCA
) =
SignedCertA = E (CertA, PvtCA)
E(CertB, PvtCA) = SignedCertB

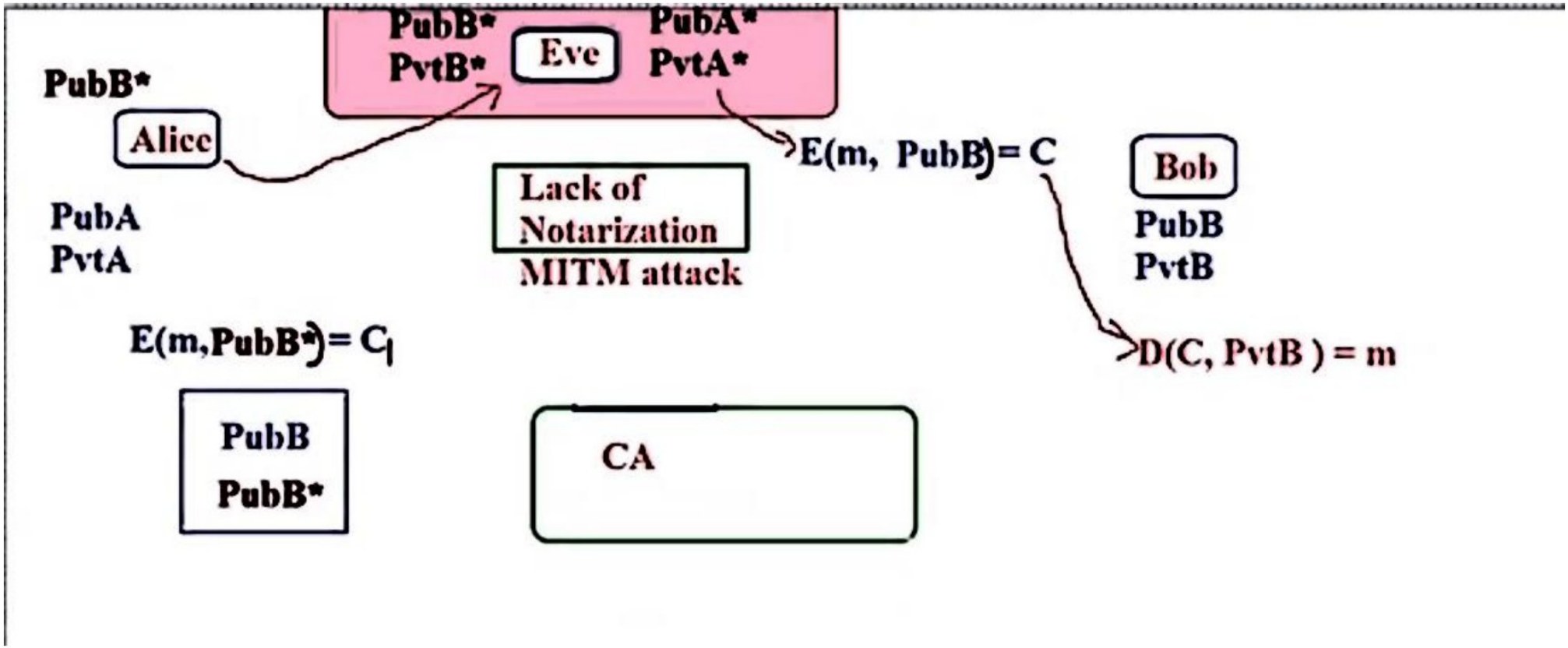

RootCA
Root
CA
PubCA
root
CertA = H(PubA)
CertB = H(PubB)
CSR
Certificate Signing
Request
CA
PubCA
PvtCA
) =
E(CertB, PvtCA) = SignedCertB
SignedCertA = E (CertA, PvtCA)

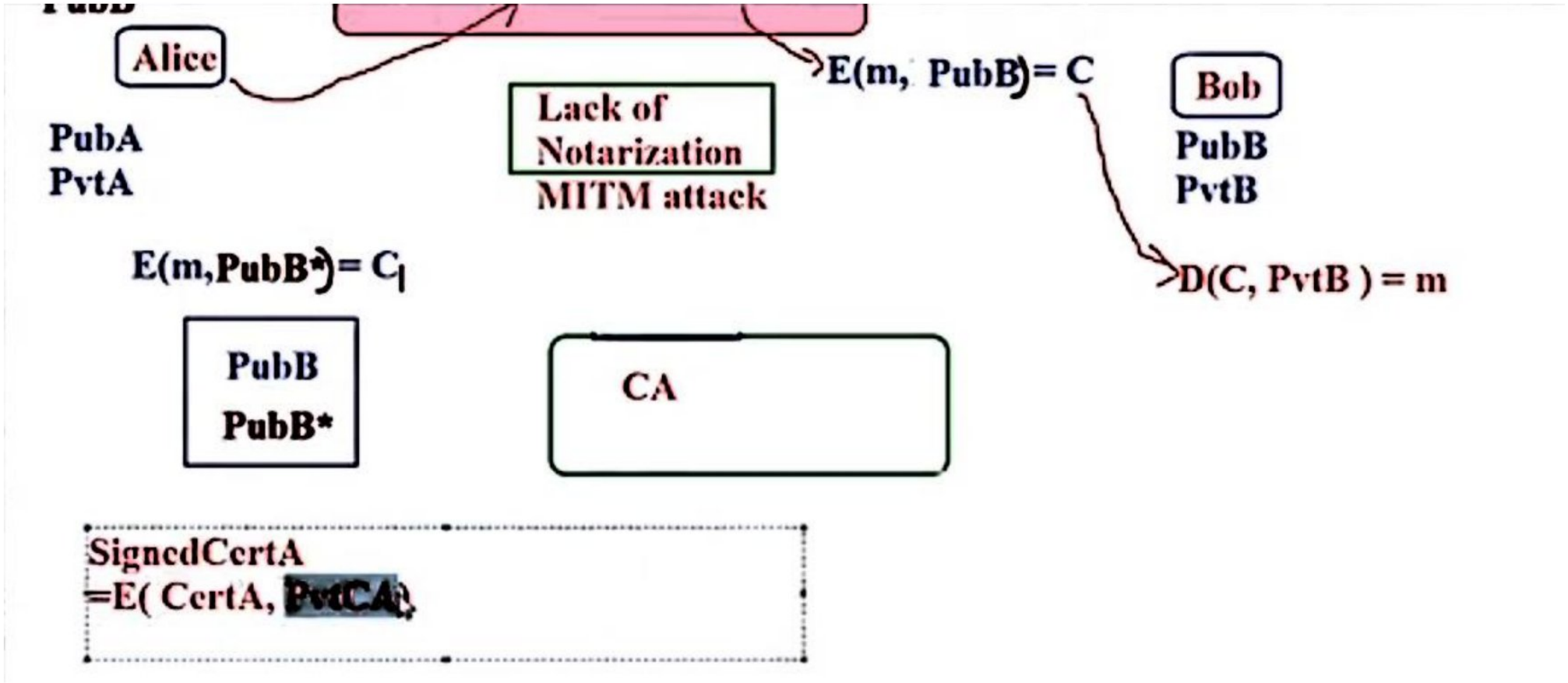

RootCA
Root
CA
CSR
CSR
CertA = H(PubA)
CertB = H(PubB)
Certificate Signing
Request
CA
PubCA
PvtCA
PubCA
PvtCA
root
root
SignedCertA = E (CertA, PvtCA)
E(CertB, PvtCA) = SignedCertB

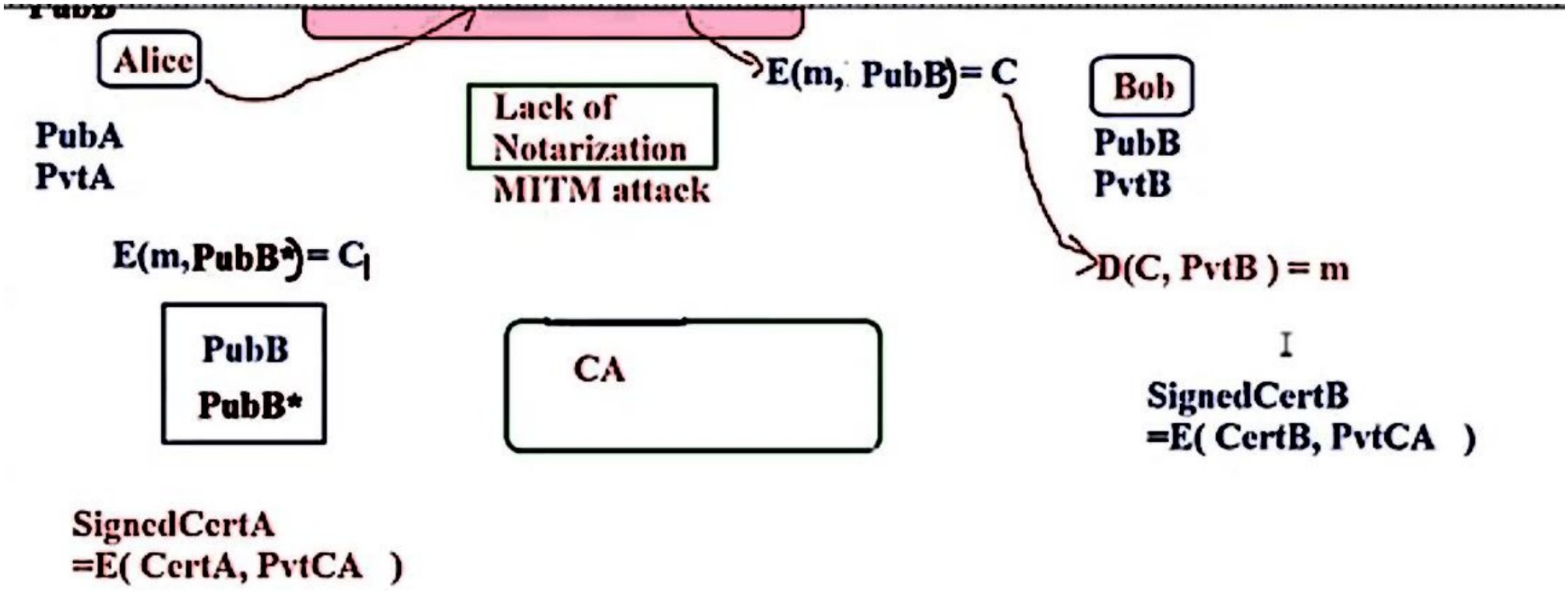

RootCA
CSR
Root
CA
CSR
CA
A)
B)
Certificate Signing
Request
PubCA
PvtCA
PubCA
PvtCA
E(CertCA, PvtCA)
E(CertB, PvtCA) = SignedCertB
(CertA, PvtCA)

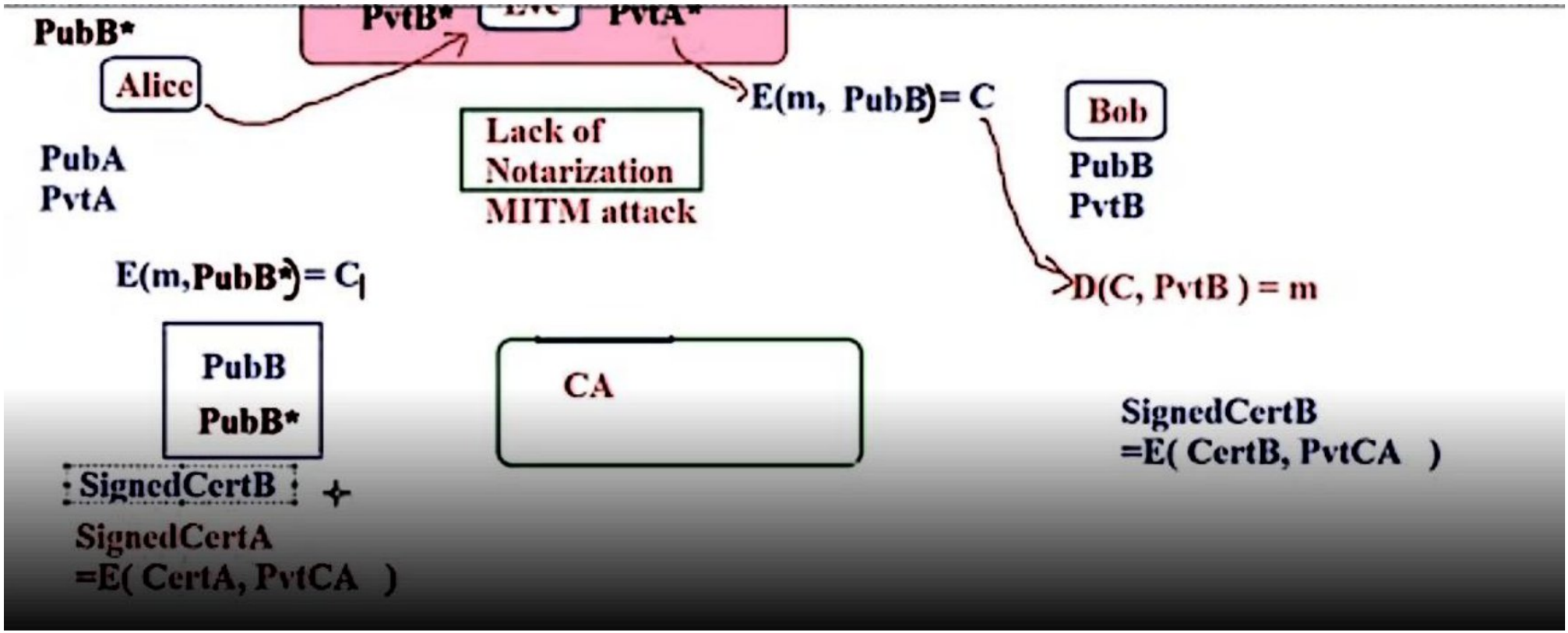

RootCA
CSR
Root
CA
CSR
A)
B)
Certificate Signing
Request
CA
PubCA
PvtCA
PubCA
PvtCA
E(CertCA, PvtCA)= SignedCertCA
E(CertB, PvtCA) = SignedCertB
(CertA, PvtCA)

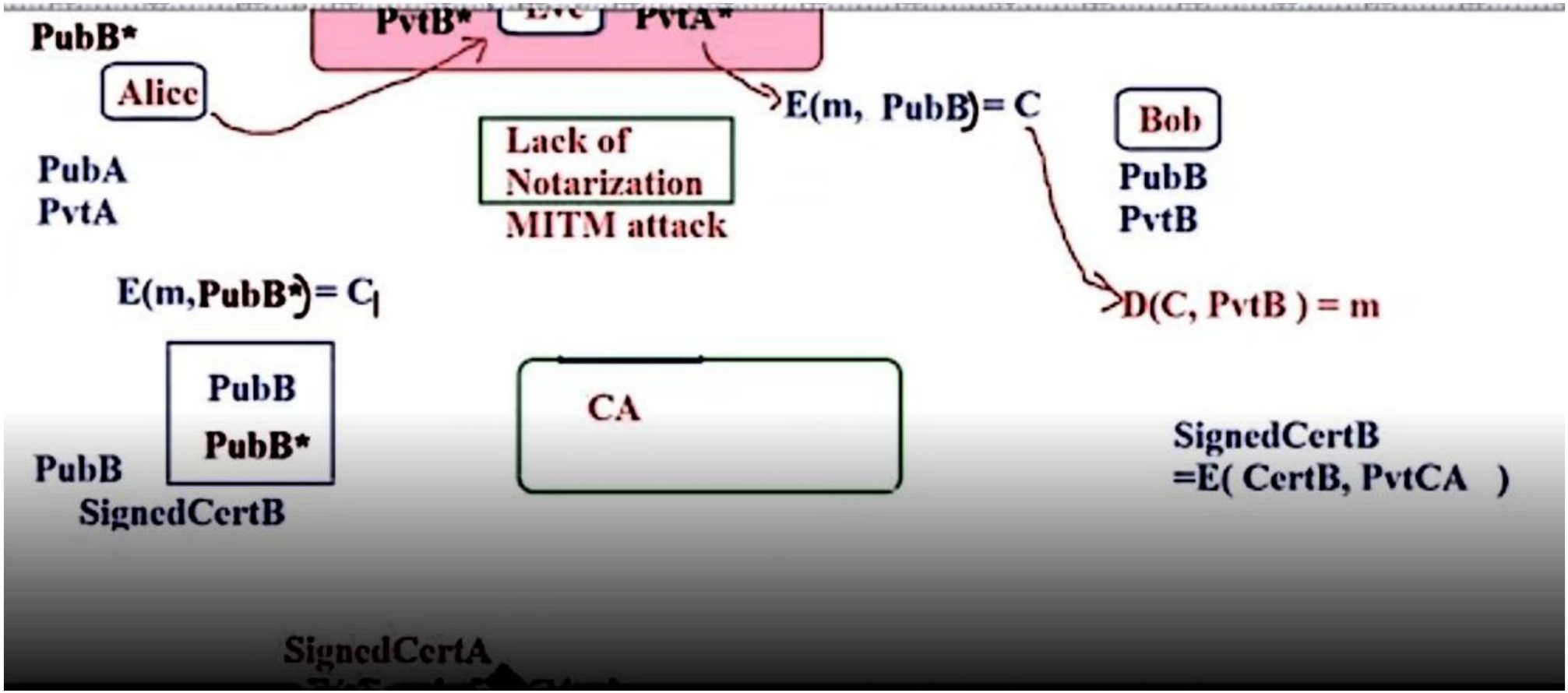

CSR
A)
B)
Certificate Signing Request
CA
PubCA
PvtCA
CSR
Root CA
PubCA
PvtCA
E(CertCA, PvtCA) = SignedCertCA
E(CertB, PvtCA) = SignedCertB
(CertA, PvtCA)

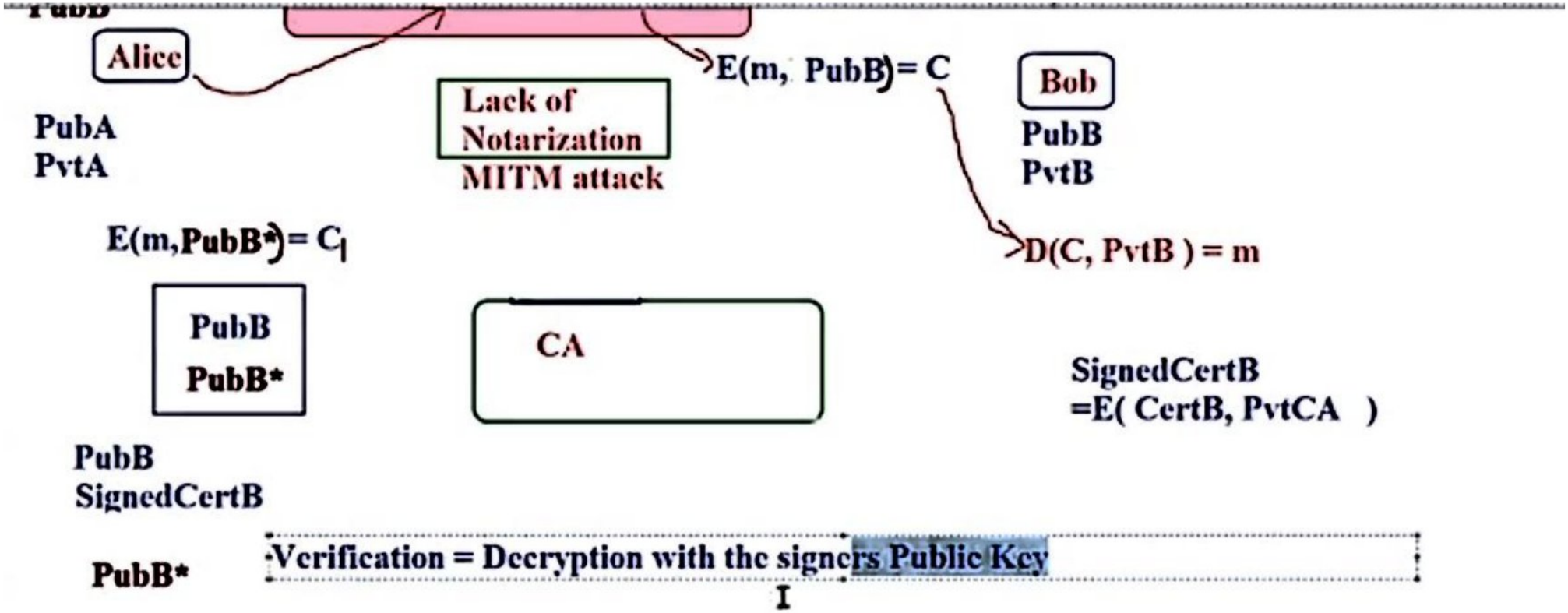

PubB*
PvtB*
Eve
PubA*
PvtA*
PubB*
Alice
E(m, PubB) = C
Bob
PubB
PvtB
PubA
PvtA
Lack of
Notarization
MITM attack
D(C, PvtB) = m
E(m,PubB*) = C
PubB
PubB*
CA

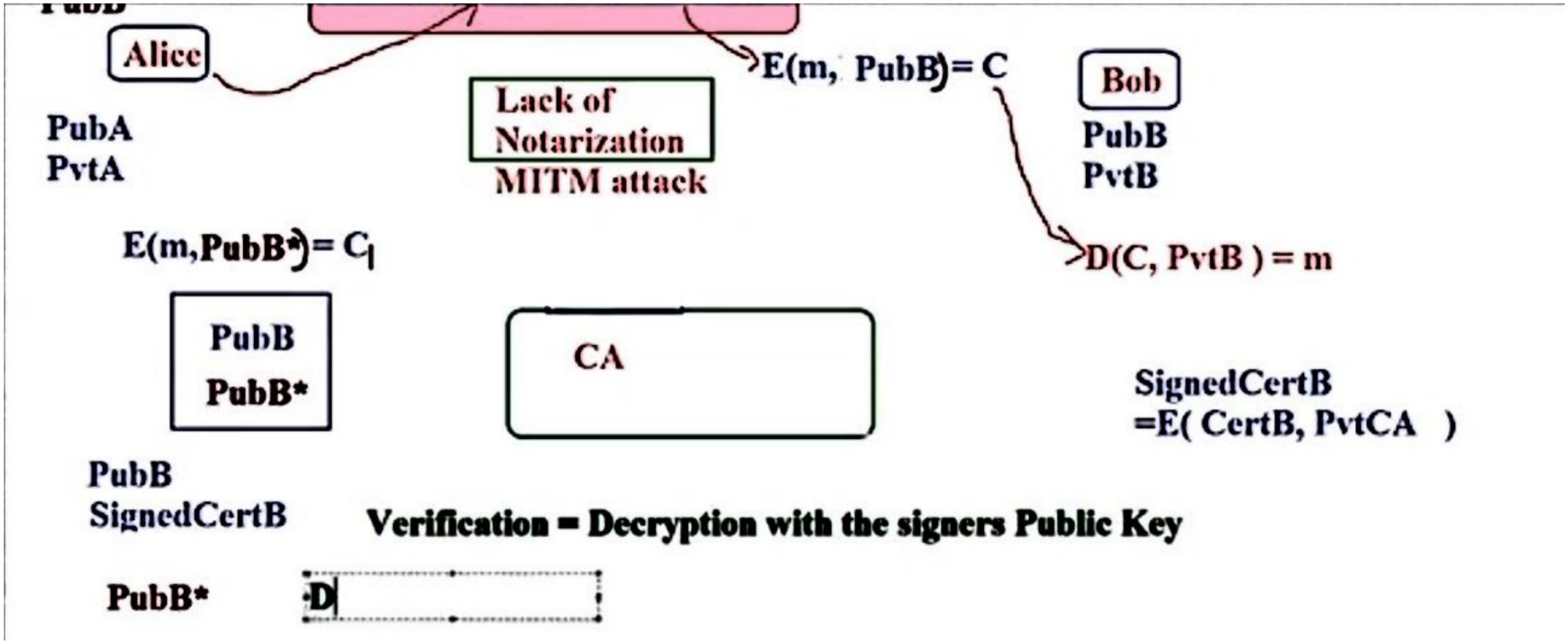

Alice
PubA
PvtA
Lack of
Notarization
MITM attack
E(m, PubB)= C
Bob
PubB
PvtB
D(C, PvtB) = m
E(m,PubB*)= C1
PubB
PubB*
CA
SignedCertA
=E(CertA, PvtCA)

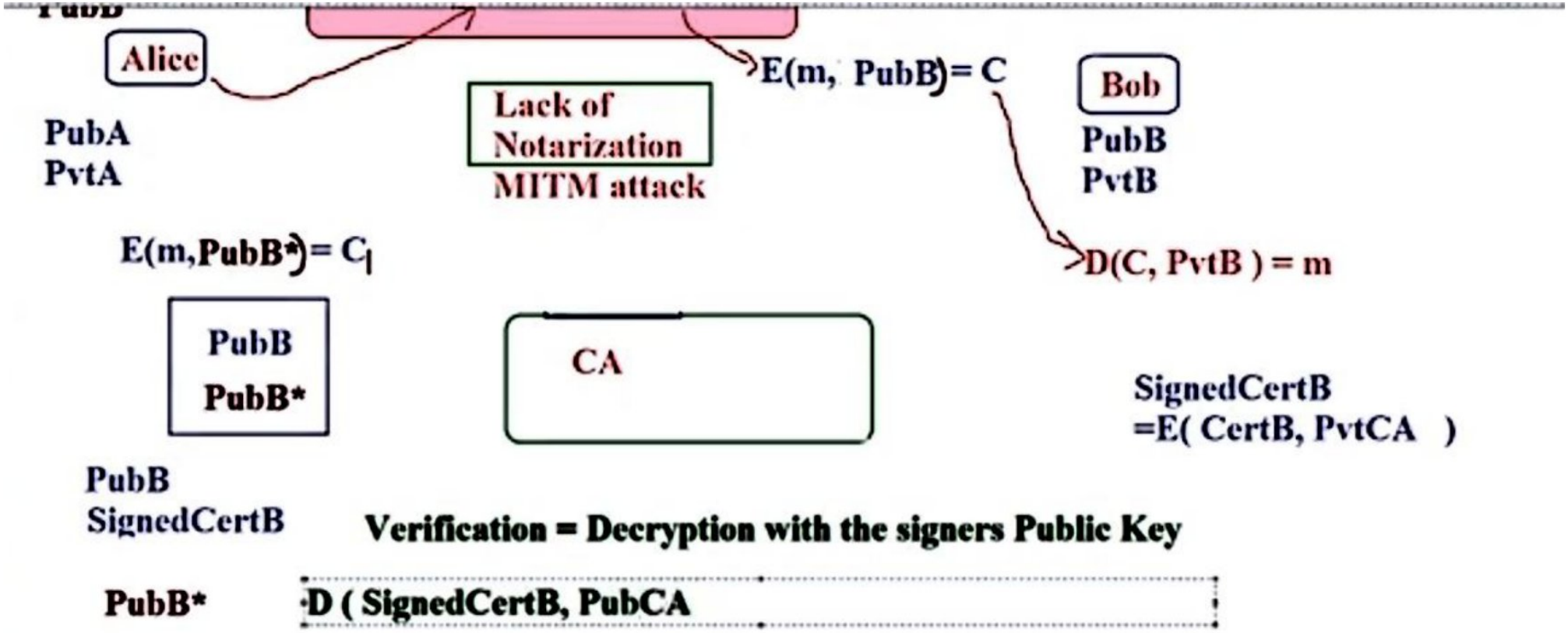

Alice
PubA
PvtA
E(m, PubB)= C
Lack of
Notarization
MITM attack
Bob
PubB
PvtB
E(m,PubB*)= C1
D(C, PvtB) = m
PubB
PubB*
CA
SignedCertB
=E(CertB, PvtCA)
SignedCertA
=E(CertA, PvtCA)

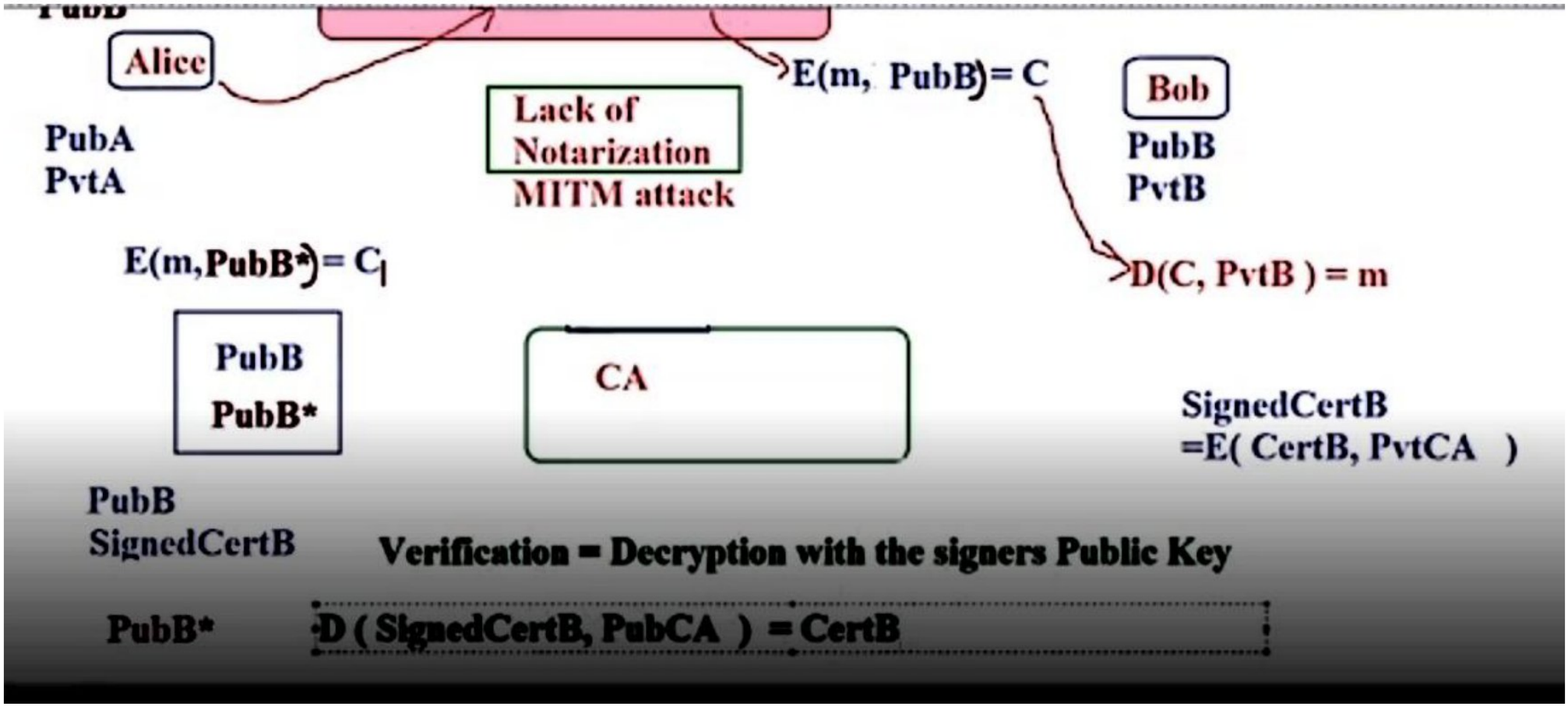

PubB*
PvtB*
PvtA*
Alice
E(m, PubB)= C
Bob
PubA
PvtA
Lack of
Notarization
MITM attack
PubB
PvtB
E(m,PubB*)= C
D(C, PvtB) = m
PubB
PubB*
CA
SignedCertB
=E(CertB, PvtCA)
SignedCertB
SignedCertA
=E(CertA, PvtCA)

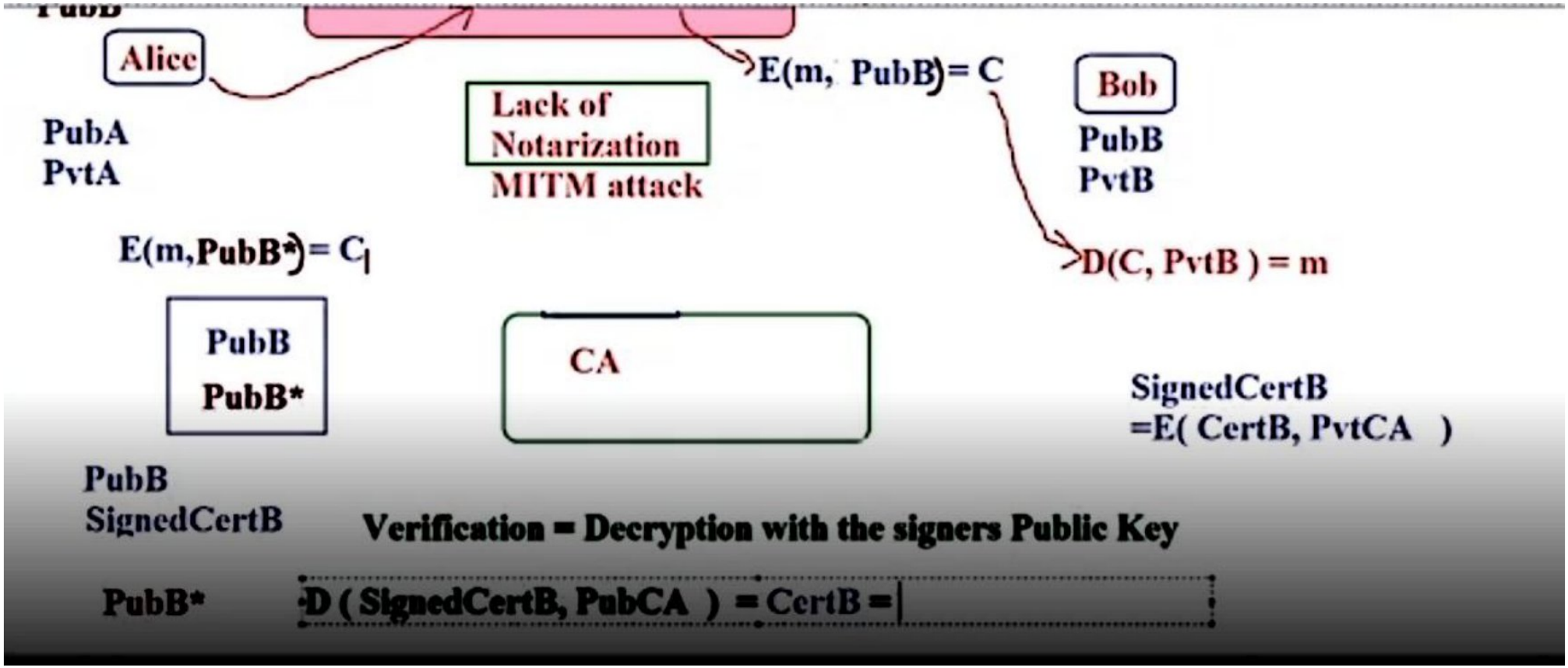

PubB*
PvtB*
PvtA*
Alice
PubA
PvtA
E(m, PubB) = C
Lack of
Notarization
MITM attack
Bob
PubB
PvtB
E(m,PubB*) = C1
D(C, PvtB) = m
PubB
PubB*
PubB
SignedCertB
CA
SignedCertB
=E(CertB, PvtCA)
SignedCertA


Alice
PubA
PvtA
E(m, PubB)= C
Lack of
Notarization
MITM attack
Bob
PubB
PvtB
E(m,PubB*)= C1
D(C, PvtB) = m
PubB
PubB*
CA
SignedCertB
=E(CertB, PvtCA)
PubB
SignedCertB
PubB*
Verification = Decryption with the signers Public Key


Alice
PubA
PvtA
E(m, PubB)= C
Lack of
Notarization
MITM attack
Bob
PubB
PvtB
E(m,PubB*)= C1
D(C, PvtB) = m
PubB
PubB*
CA
SignedCertB
=E(CertB, PvtCA)
PubB
SignedCertB
Verification = Decryption with the signers Public Key
PubB*
D


Alice
PubA
PvtA
E(m, PubB)= C
Lack of
Notarization
MITM attack
Bob
PubB
PvtB
E(m,PubB*)= C1
D(C, PvtB) = m
PubB
PubB*
CA
SignedCertB
=E(CertB, PvtCA)
PubB
SignedCertB
Verification = Decryption with the signers Public Key
PubB*
D (SignedCertB, PubCA


Alice
PubA
PvtA
E(m, PubB)= C
Lack of
Notarization
MITM attack
Bob
PubB
PvtB
E(m,PubB*)= C
D(C, PvtB) = m
PubB
PubB*
CA
SignedCertB
=E(CertB, PvtCA)
PubB
SignedCertB
Verification = Decryption with the signers Public Key
PubB*
D (SignedCertB, PubCA) = CertB


Alice
PubA
PvtA
E(m, PubB)= C
Lack of
Notarization
MITM attack
Bob
PubB
PvtB
E(m,PubB*)= C1
D(C, PvtB) = m
PubB
PubB*
CA
SignedCertB
=E(CertB, PvtCA)
PubB
SignedCertB
Verification = Decryption with the signers Public Key
PubB*
D (SignedCertB, PubCA) = CertB =

X.509 Certificates

Certificate = Hash of the public key

CertA = H(PubA)
CertB = H(PubB)

CSR

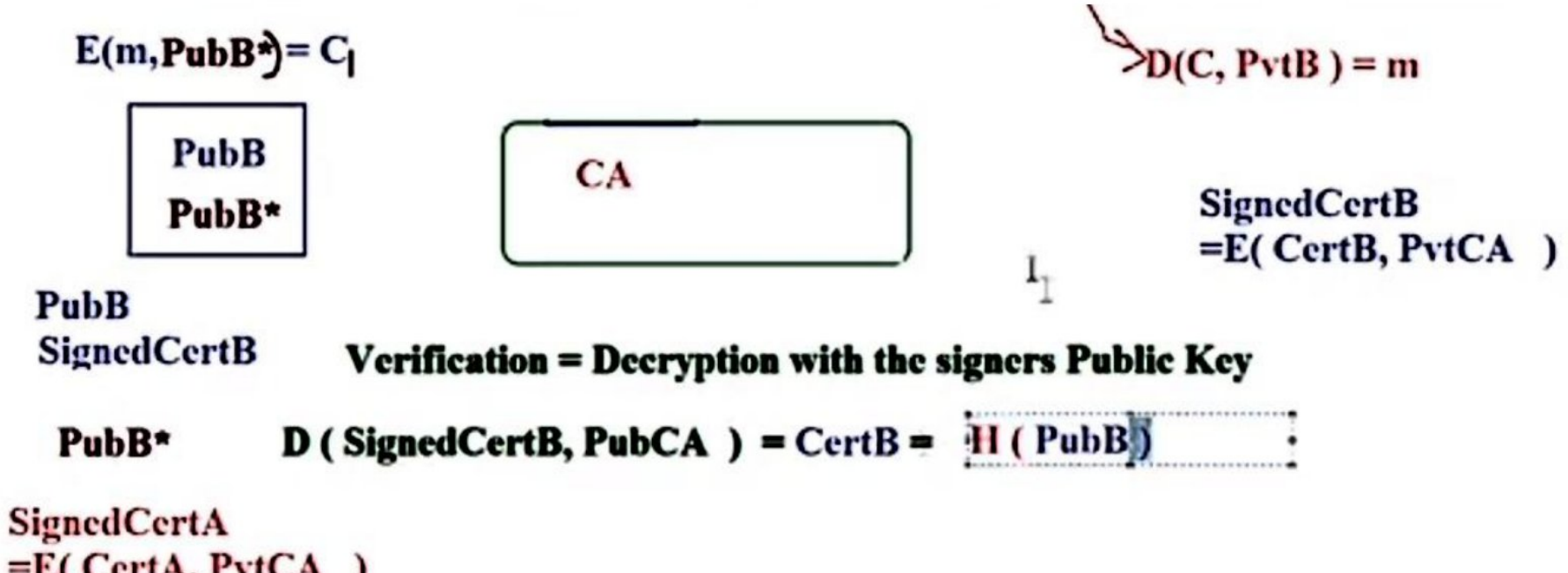
Certificate Signing Request

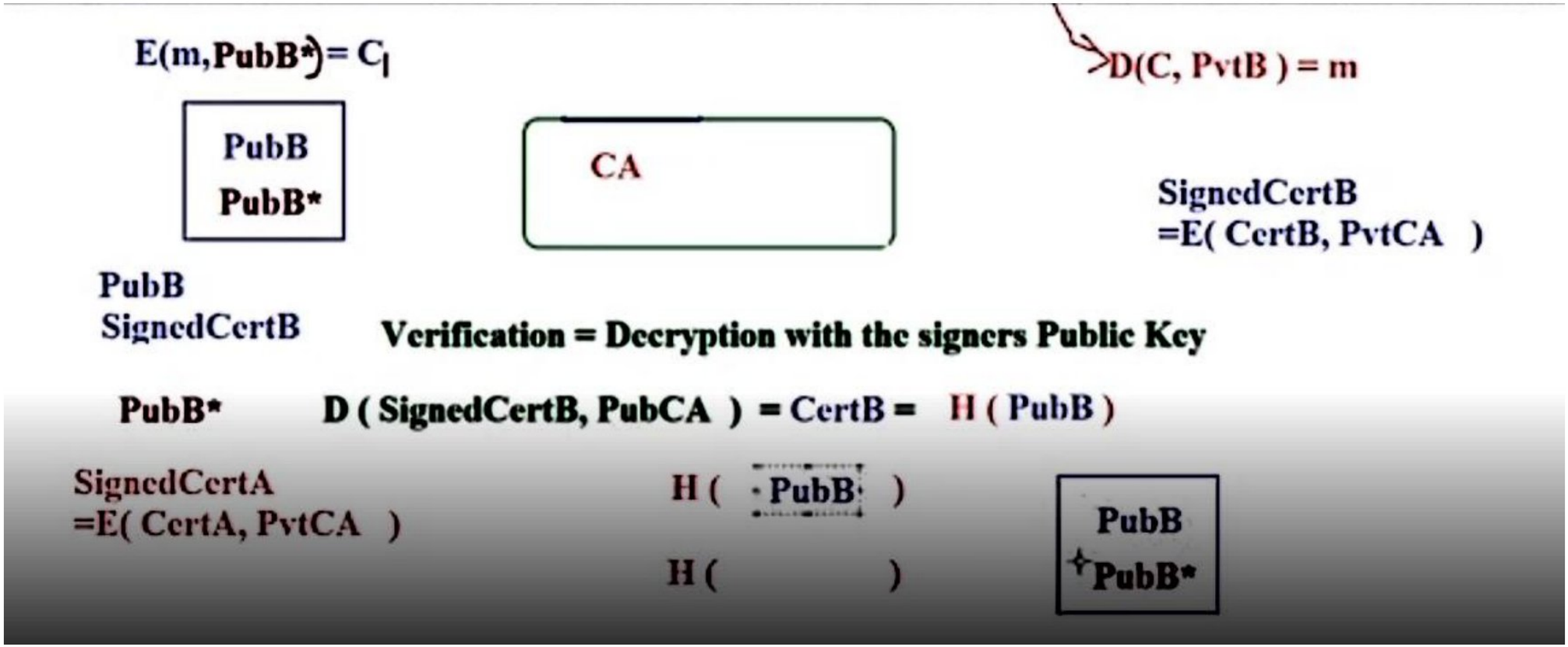
H(

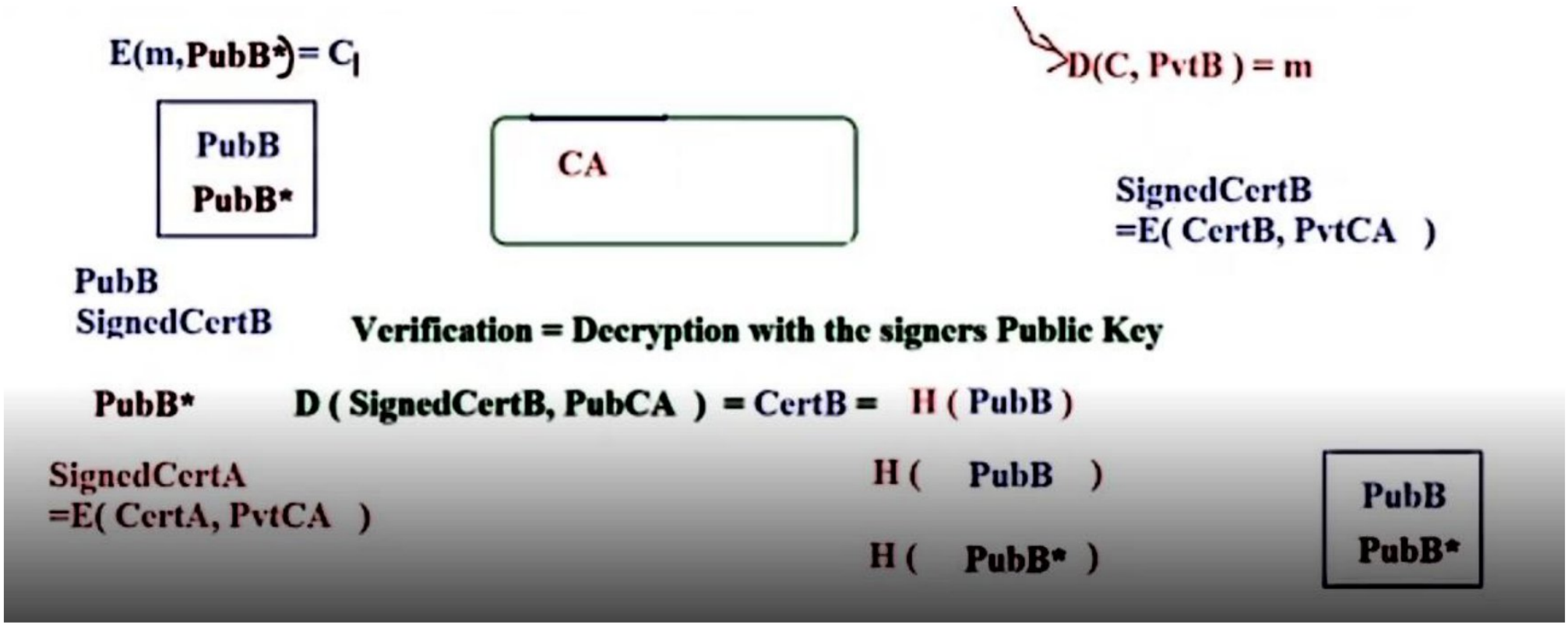
) =

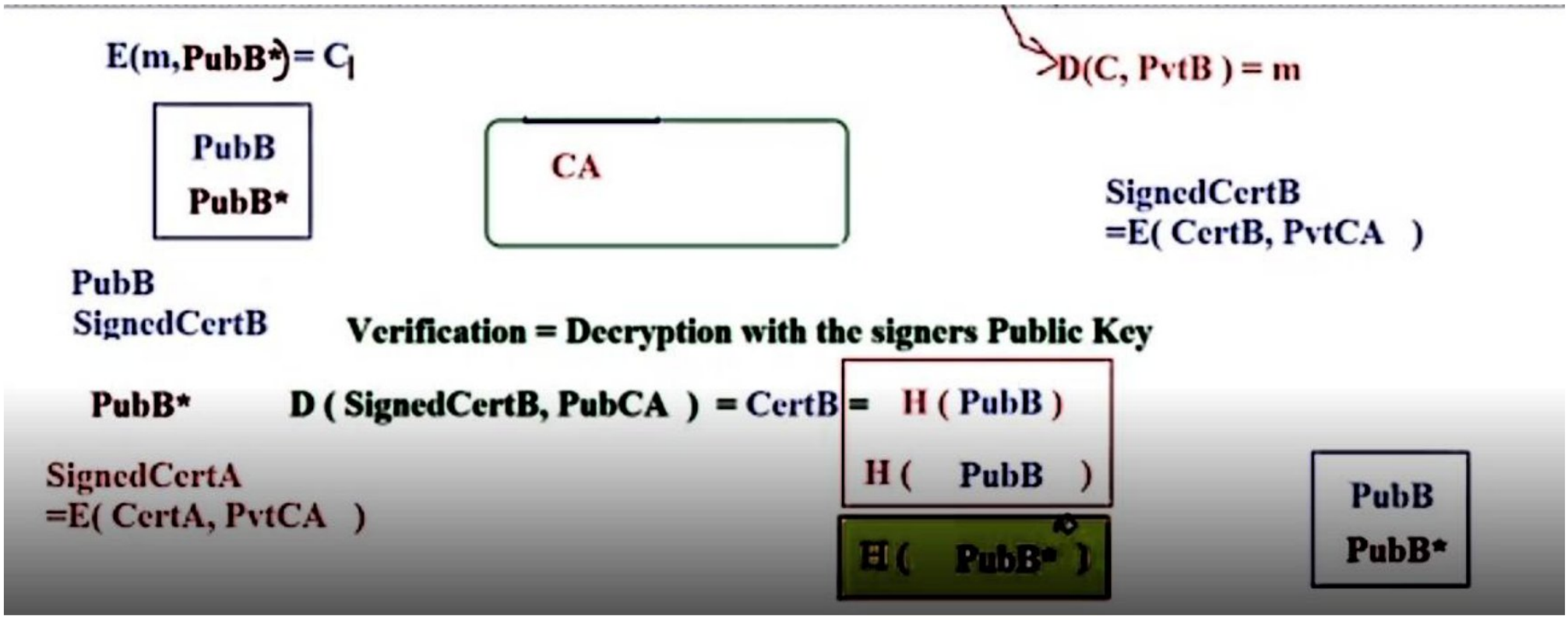
Signing = to encrypt with the private key

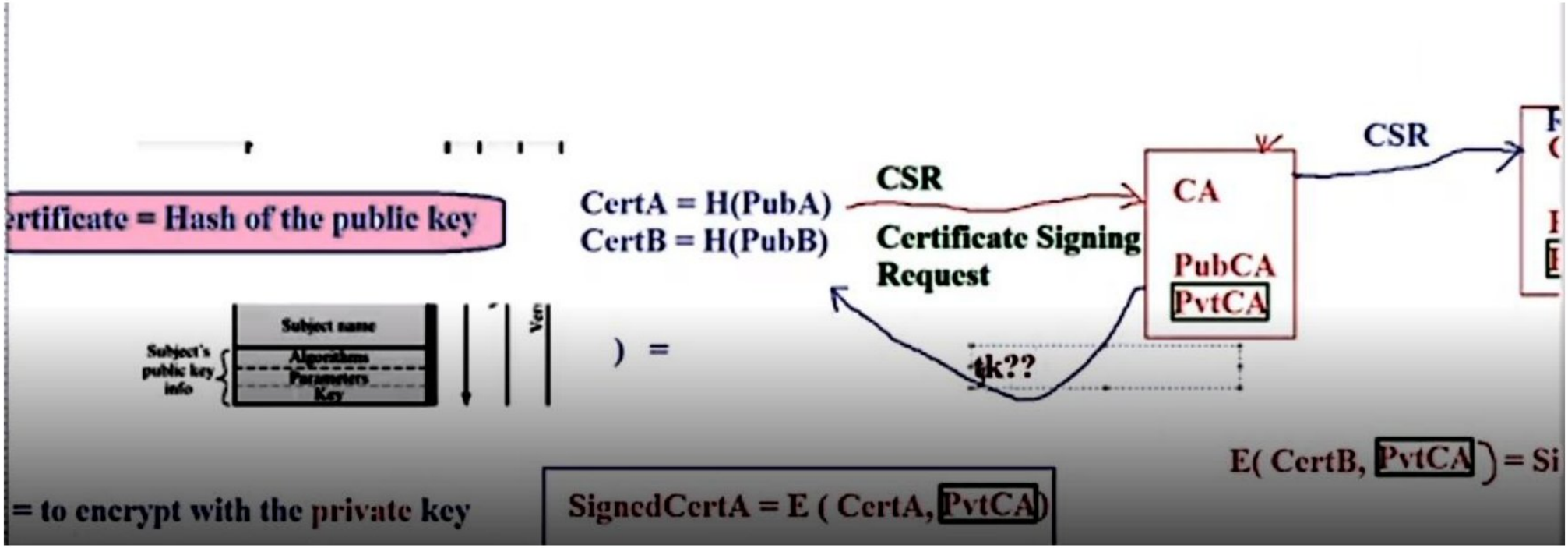
SignedCertA = E (CertA, PvtCA)


E(m,PubB*)= C
PubB
PubB*
CA
D(C, PvtB) = m
SignedCertB
=E(CertB, PvtCA)
PubB
SignedCertB
Verification = Decryption with the signers Public Key
PubB*
D (SignedCertB, PubCA) = CertB =
H (PubB)
SignedCertA
=E(CertA, PvtCA)


E(m,PubB*)= C
D(C, PvtB) = m
PubB
PubB*
CA
SignedCertB
=E(CertB, PvtCA)
PubB
SignedCertB
Verification = Decryption with the signers Public Key
PubB*
D (SignedCertB, PubCA) = CertB = H (PubB)
SignedCertA
=E(CertA, PvtCA)
H (PubB)
H ( )
PubB
PubB*


E(m,PubB*)= C
D(C, PvtB) = m
PubB
PubB*
CA
SignedCertB
=E(CertB, PvtCA)
PubB
SignedCertB
Verification = Decryption with the signers Public Key
PubB*
D (SignedCertB, PubCA) = CertB = H (PubB)
SignedCertA
=E(CertA, PvtCA)
H (PubB)
H (PubB*)
PubB
PubB*


E(m,PubB*)= C
D(C, PvtB) = m
PubB
PubB*
CA
SignedCertB
=E(CertB, PvtCA)
PubB
SignedCertB
Verification = Decryption with the signers Public Key
PubB*
D (SignedCertB, PubCA) = CertB
H (PubB)
H (PubB)
H (PubB*)
SignedCertA
=E(CertA, PvtCA)
PubB
PubB*


rtificate = Hash of the public key
CertA = H(PubA)
CertB = H(PubB)
CSR
Certificate Signing Request
CA
PubCA
PvtCA
CSR
Subject name
Subject's public key info
Algorithms
Parameters
Key
) =
tk??
E(CertB, PvtCA) = Si
= to encrypt with the private key
SignedCertA = E (CertA, PvtCA)

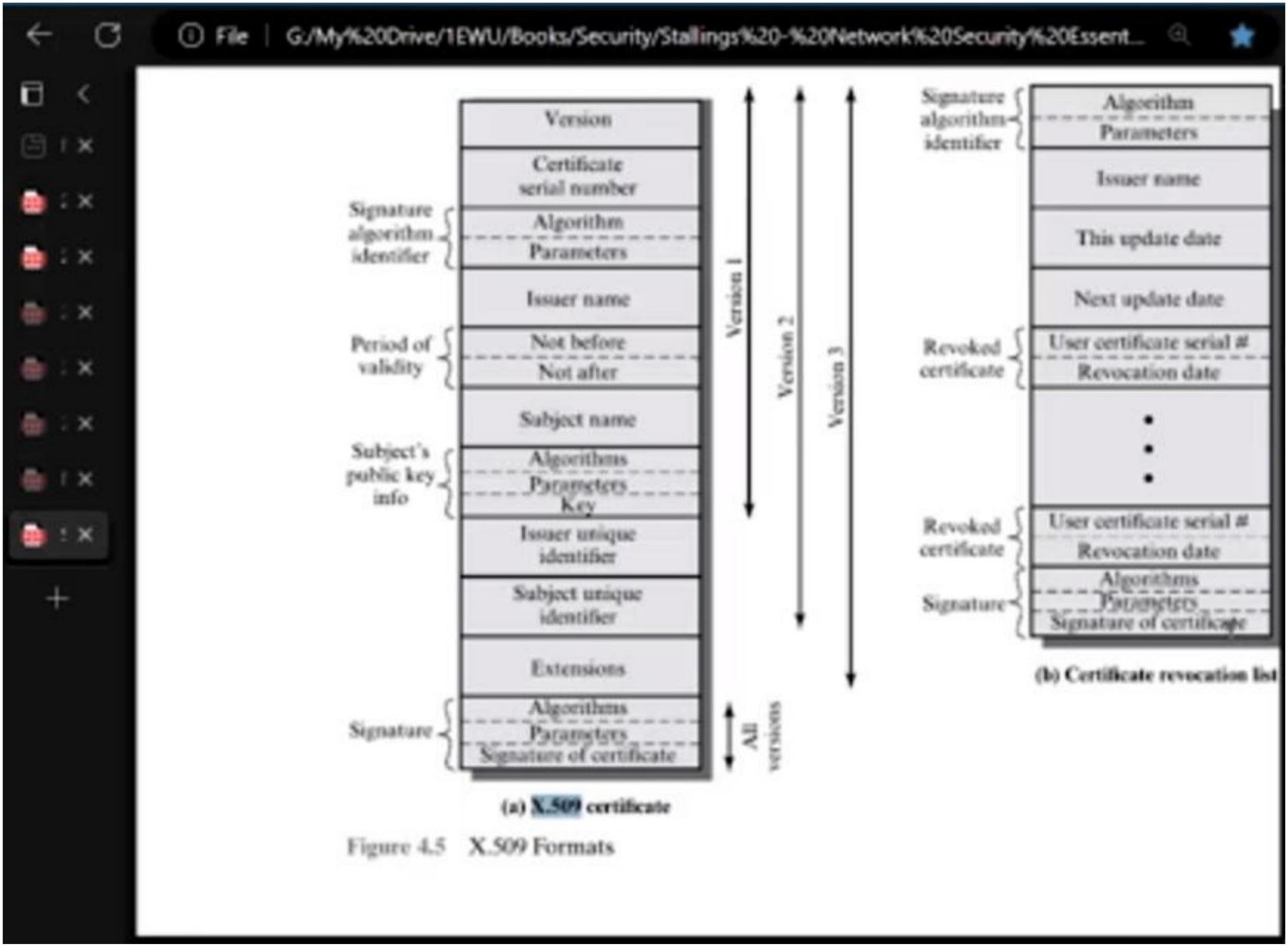
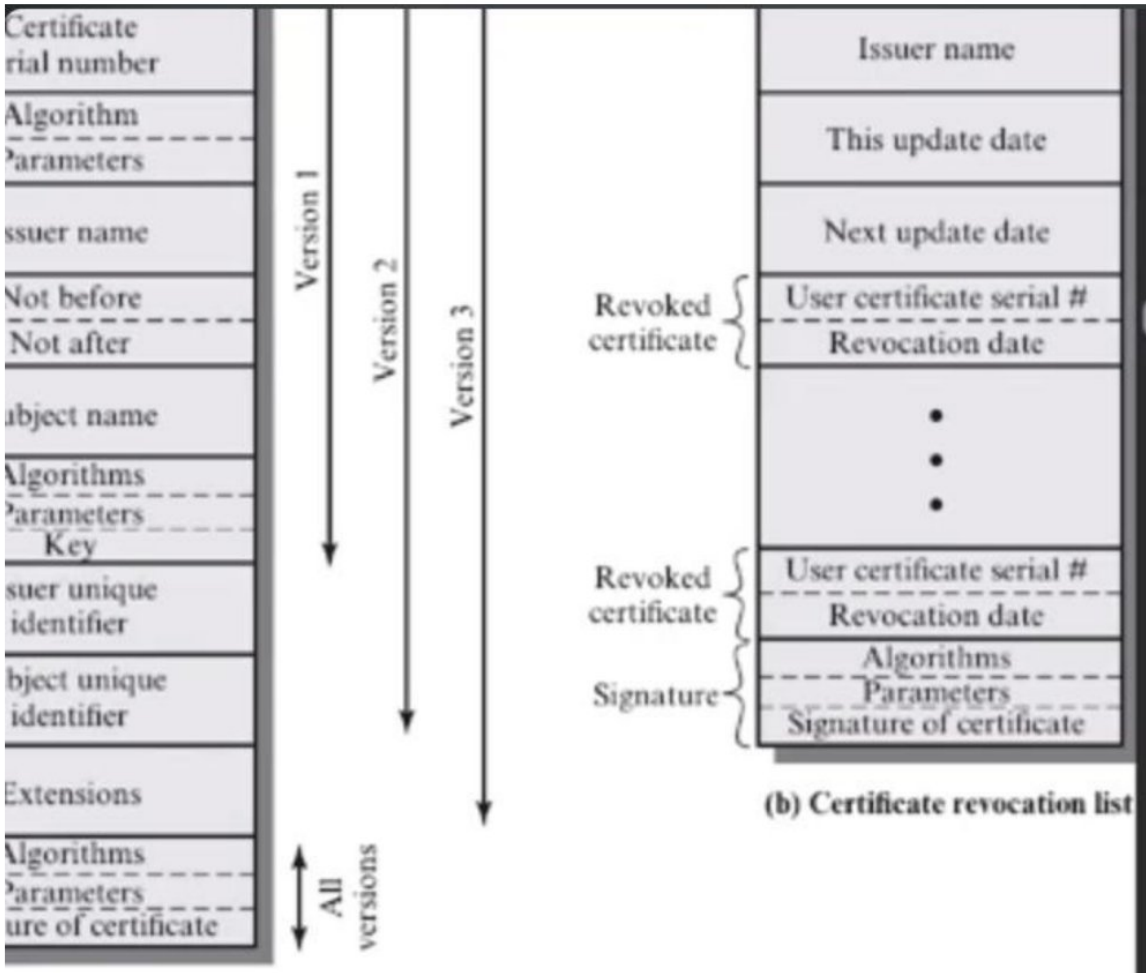


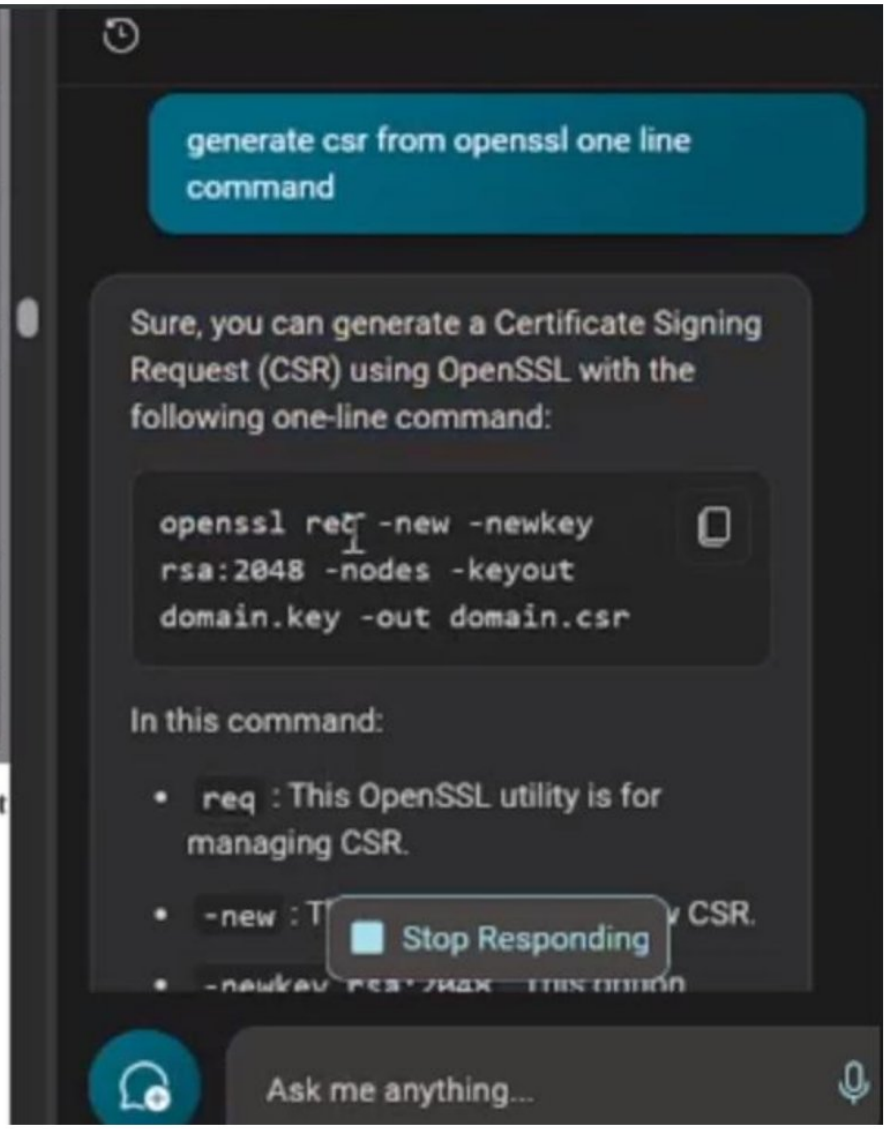
Figure 4.5 X.509 Formats

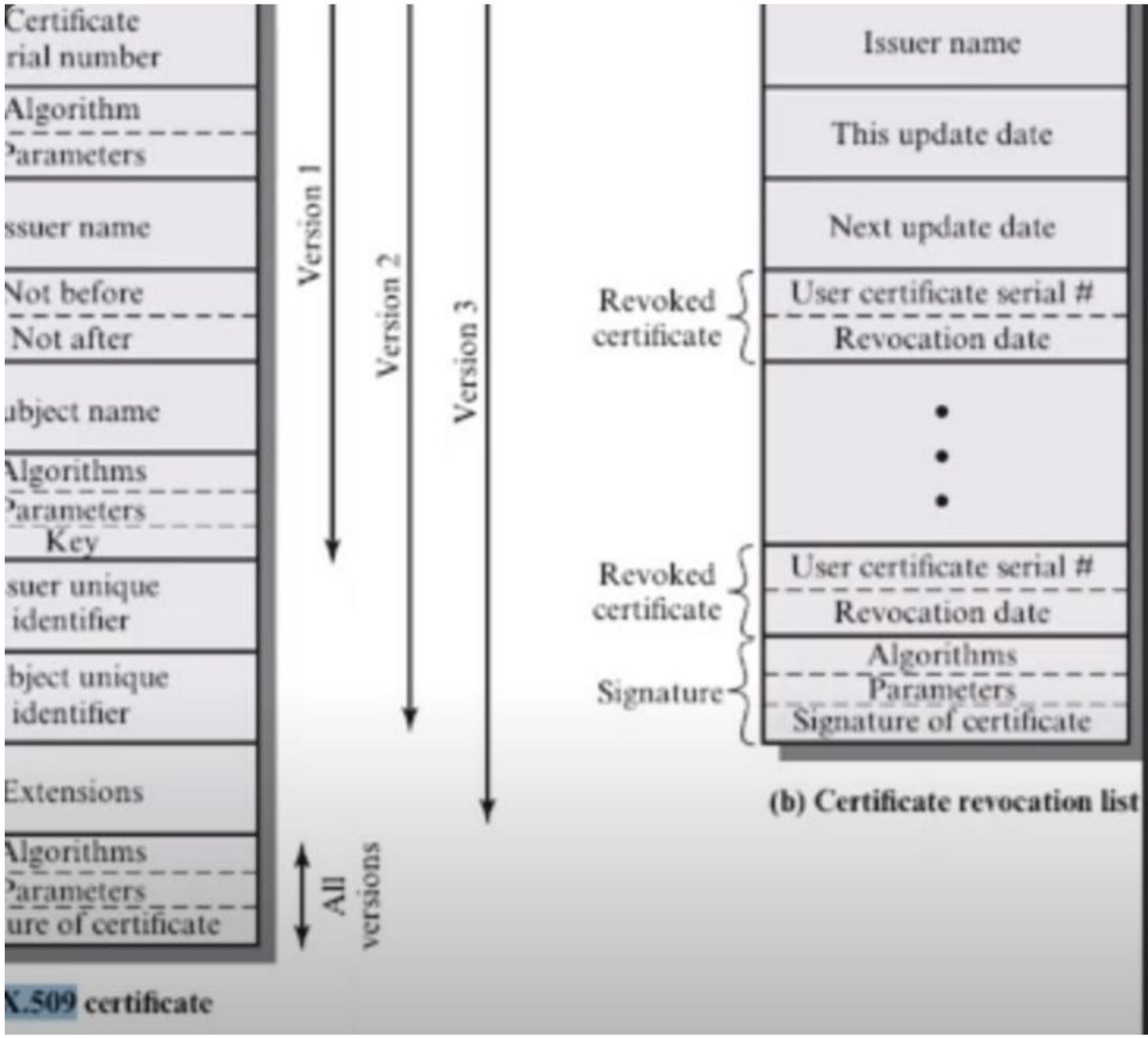


(b) Certificate revocation list

.509 certificate

Formats





Generating CSR using OpenSSL

In this command:

- `req` : This OpenSSL utility is for managing CSR.
- `-new` : This option creates a new CSR.
- `-newkey rsa:2048` : This option creates a new RSA key of 2048 bits.
- `-nodes` : This option ensures that the private key is not encrypted with a pass phrase.
- `-keyout domain.key` : This option specifies the filename to write the newly created private key to.
- `-out domain.csr` : This option specifies the output filename to write the CSR to.

tificates issued by that CA, including both those issued to users and to other CAs. These lists also should be posted on the directory.

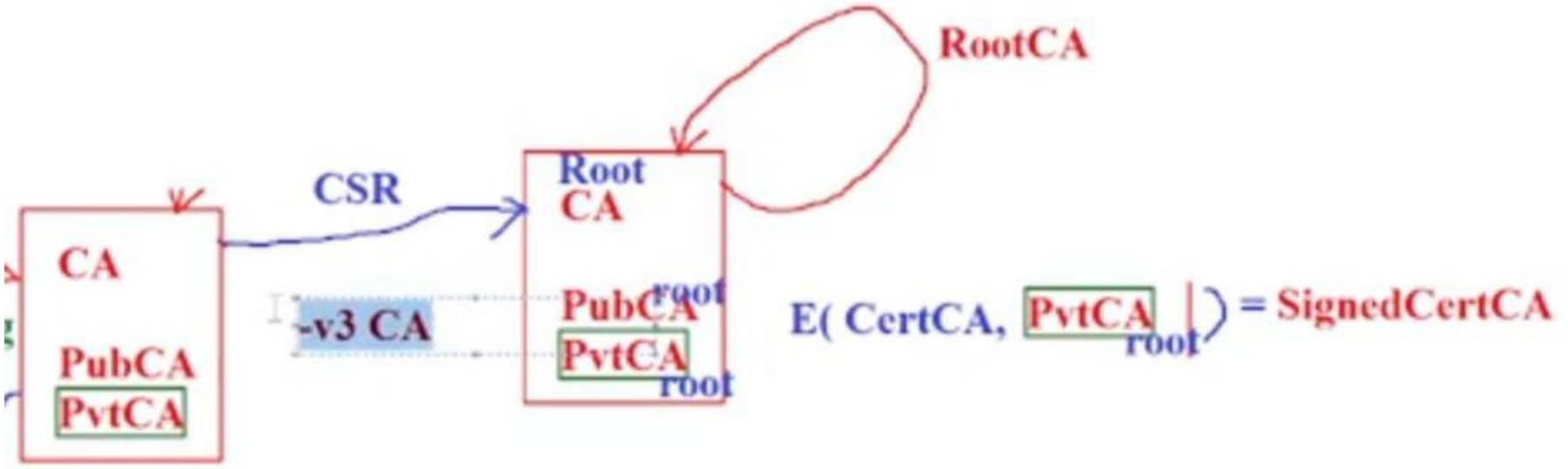
Each certificate revocation list (CRL) posted to the directory is signed by the issuer and includes (Figure 4.5b) the issuer's name, the date the list was created, the date the next CRL is scheduled to be issued, and an entry for each revoked certificate. Each entry consists of the serial number of a certificate and revocation date for that certificate. Because serial numbers are unique within a CA, the serial number is sufficient to identify the certificate.

When a user receives a certificate in a message, the user must determine whether the certificate has been revoked. The user could check the directory each time a certificate is received. To avoid the delays (and possible costs) associated with directory searches, it is likely that the user would maintain a local cache of certificates and lists of revoked certificates.

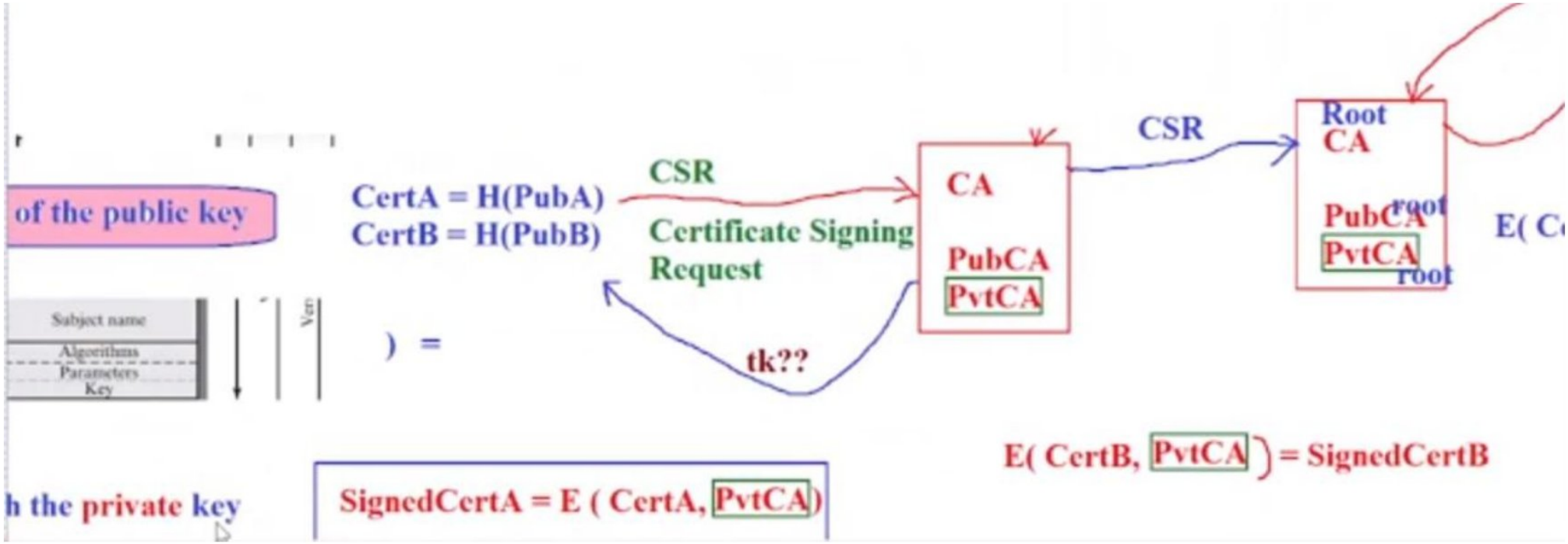
X.509 Version 3

The X.509 version 2 format does not convey all of the information that recent design and implementation experience has shown to be needed. [FORD95] lists the following requirements not satisfied by version 2:

1. The Subject field is inadequate to convey the identity of a-key owner to a public-key user. X.509 names may be relatively short and lacking in obvious identification details that may be needed by the user.



E(CertB, PvtCA) = SignedCertB


of the public key
CertA = H(PubA)
CertB = H(PubB)
CSR
Certificate Signing Request
CA
PubCA
PvtCA
CSR
Root CA
PubCA
PvtCA
root
root
tk??
Subject name
Algorithms
Parameters
Key
) =
h the private key
SignedCertA = E (CertA, PvtCA)
E(CertB, PvtCA) = SignedCertB
E(C

Level, Mark, and Level of Complex Engineering Problems for each question are mentioned at the right margin.

Q1. *a.* **Explain** the different types of attack surface and provide examples of each type. [05] **[CO1, C3, Mark: 10]**

b. Consider a mobile banking interface in which the users provide their mobile phone numbers and a personal identification number (PIN) for account access. **Develop** an attack tree for this kind of system. [05] **[EP1, EP2]**

Q2. **Decode** the given text to Base64. Use the tables are given in the next page. **CO1, C3, Mark: 05]**

U2VDdVJpVHk=

Q3. *a.* **Explain** the issues related to symmetric encryption. [02] **[CO1, C3, Mark: 05]**

b. **Demonstrate** a hybrid protocol that uses both symmetric and asymmetric encryptions, with the help of a diagram and appropriate mathematical notations. [03] **[EP1, EP2, EP4]**

Q4. *a.* **Demonstrate** a *Diffie-Hellman Key Establishment* between Alice and Bob, **[CO2, C4,**

mobile phone numbers and a personal identification number (PIN) for account access. **Develop** an attack tree for this kind of system. [05]

Q2. **Decode** the given to Base64. Use the tables are given in the next page. **CO1, C3, Mark: 05]**

U2VDdVJpVHk=

Q3. *a.* **Explain** the issue ed to symmetric encryption. [02] **[CO1, C3, Mark: 05] [EP1, EP2, EP4]**

b. **Demonstrate** a h protocol that uses both symmetric and asymmetric encryptions, with help of a diagram and appropriate mathematical notations. [03]

Q4. *a.* **Demonstrate** a *Diffie-Hellman Key Establishment* between Alice and Bob, through a clear channel where Eve is eavesdropping. Use prime numbers larger than 30. [03] **[CO2, C4, Mark: 05] [EP1, EP2]**

b. **Explain** how Eve can determine the symmetric key from the public knowledge. [02]

Q5. *a.* How a certain vulnerability of a software could be tracked? **[CO2, C2, Mark: 05] [EP1, EP2, EP4]**

b. How is *Trojan Horse* related to pirated software?

c. Differentiate between transposition cipher and substitution cipher.

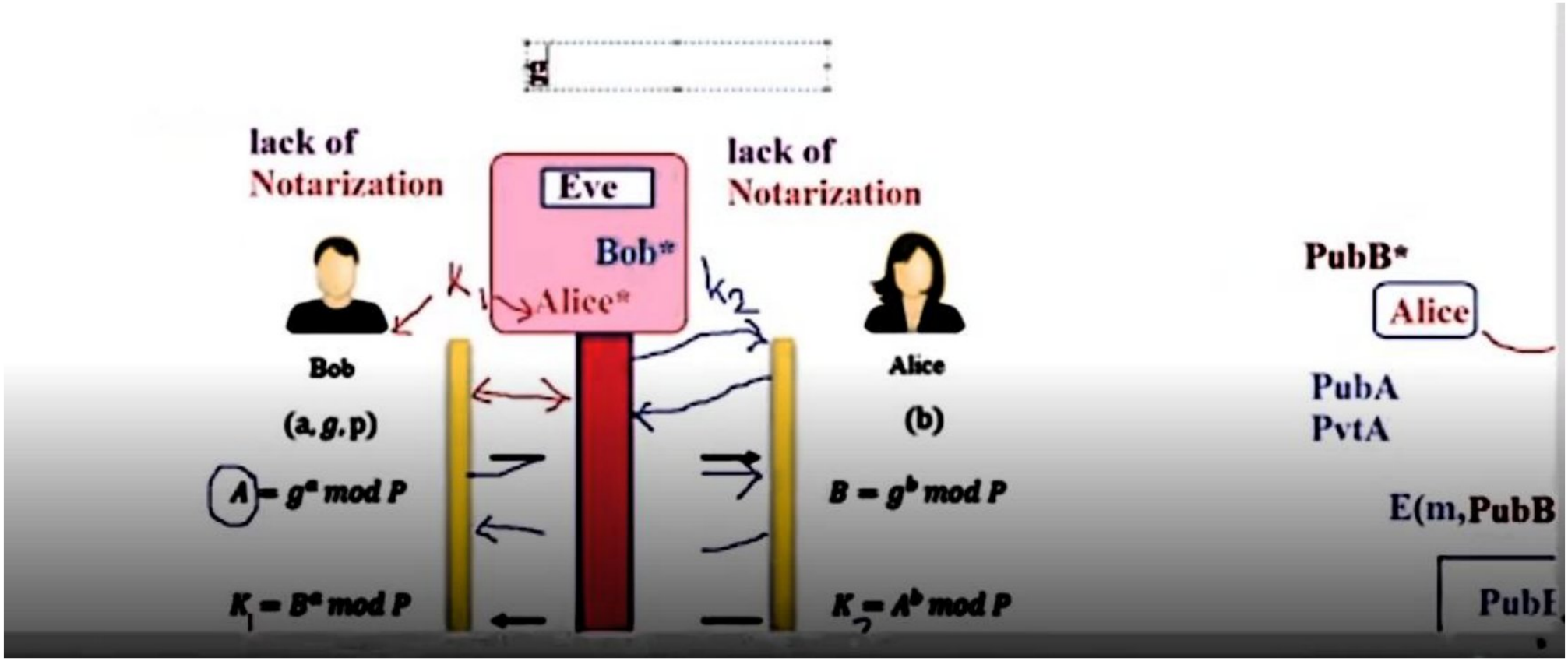
d. Explain LSB Steganography.

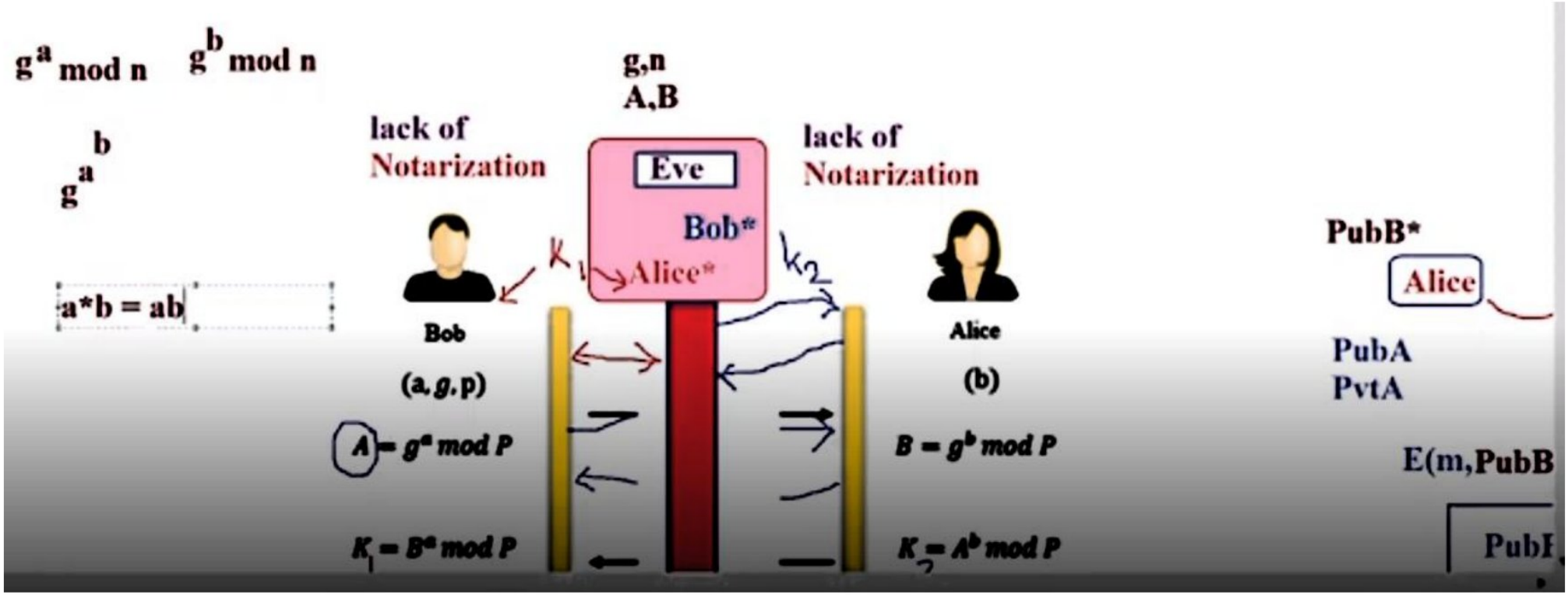
e. What are the hard problems that are the basis of modern cryptography?

f. Which software could be used to generate a wordlist?

g. Which encryptions algorithms are used in the Wi-Fi connections?

h. In the Bandit wargame, how do you proceed from one level to another?


lack of
Notarization
Eve
Bob*
Alice*
lack of
Notarization
Bob
(a, g, p)
A = g^a mod P
K1 = B^a mod P
Alice
(b)
B = g^b mod P
K2 = A^b mod P
PubB*
Alice
PubA
PvtA
E(m,PubB


$g^a \bmod n$
$g^b \bmod n$
g^{ab}
a*b = ab
g,n
A,B
lack of Notarization
Eve
Bob*
Alice*
lack of Notarization
Bob
(a, g, p)
$A = g^a \bmod P$
$K_1 = B^a \bmod P$
Alice
(b)
$B = g^b \bmod P$
$K_2 = A^b \bmod P$
PubB*
Alice
PubA
PvtA
E(m,PubB

$2^x = 8$

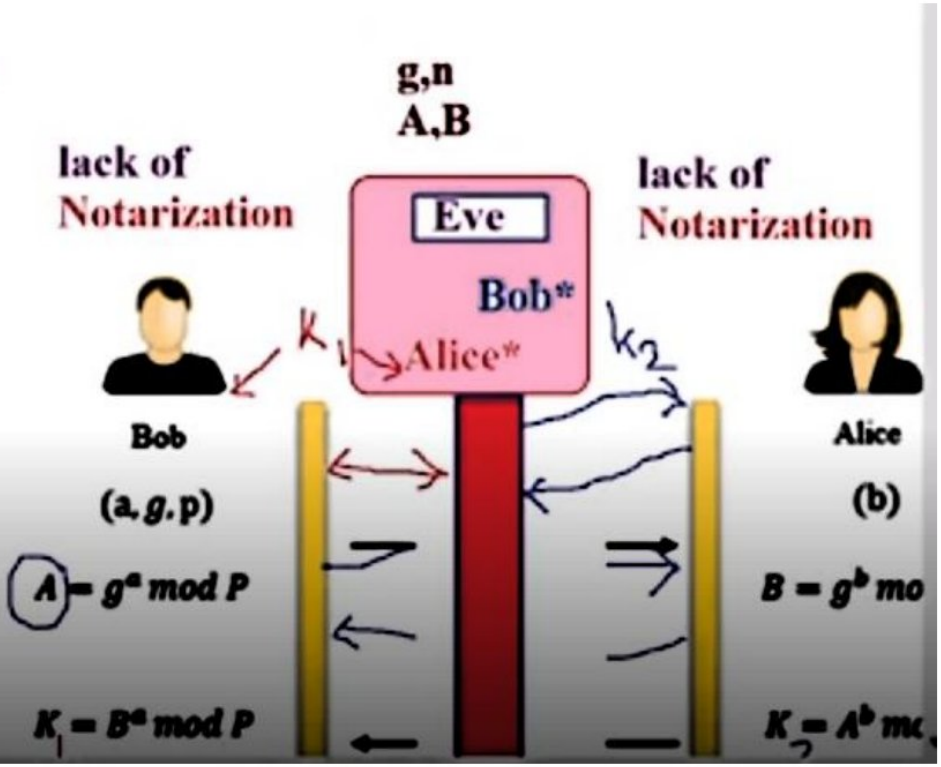
$x \log 2 = \log 8$

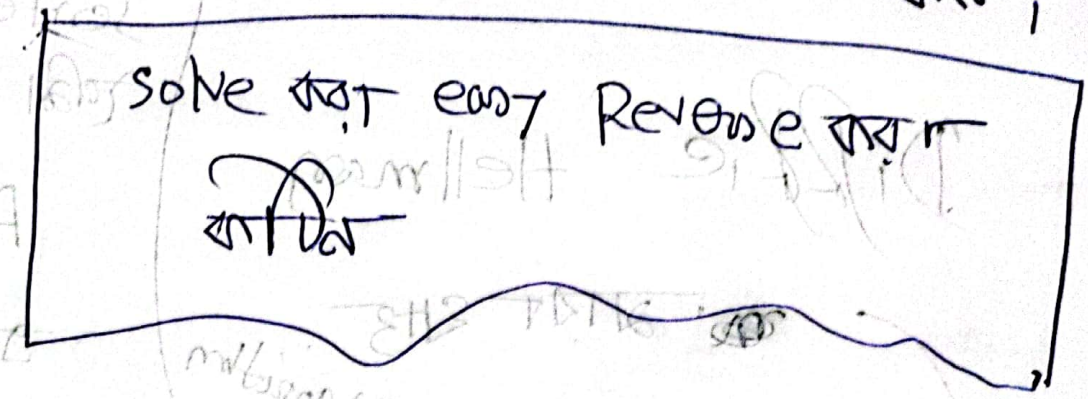
$g^a \bmod n$ $g^b \bmod n$

g^{ab}

$a*b = ab$

Discrete Logarithm Problem





NIST → standardized provide করে
ECC ভালো graph

ECC backdoor

X25519. Xargs. or

geomatric distribution

man in the middle attacks using RSA

Elliptic-curve-Diffie-Hellman

S/MIME
Base64
Transfer
Email data
Picture, video,
Image, file,
pdf

RFC

kerberos

Captcha
web করি
DDOS Attack
আটকানোর
জন্য

MSS

MTU

Home work

How to track
software vulnarabili
↓
CVE

Bandit wargame

level
Password
Collect
করতে হবে user
name change
করে level
Password

last level
- private key file
location
input করে

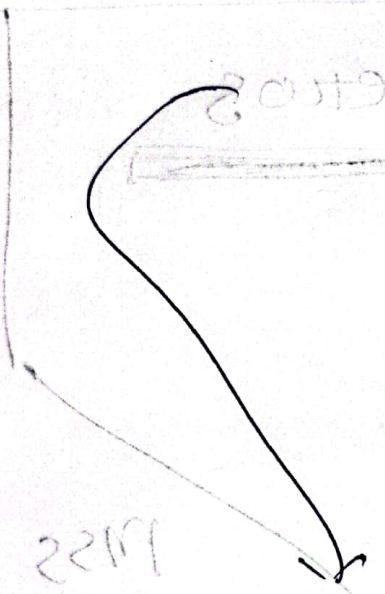
half open connection

↓

Syn (good morning)

student good morning

তারপর কোন হ্যান্ড শেক নাই



3 way connection

DOS attack

on seq hold attack

Network Security and essentials 4th edition

Theme: Page - 123

Date: / /

☐Sat ☐Sun ☐Mon ☐Tue ☐wed ☐Thu ☐Fri

Realm

kerberos → wikipedia

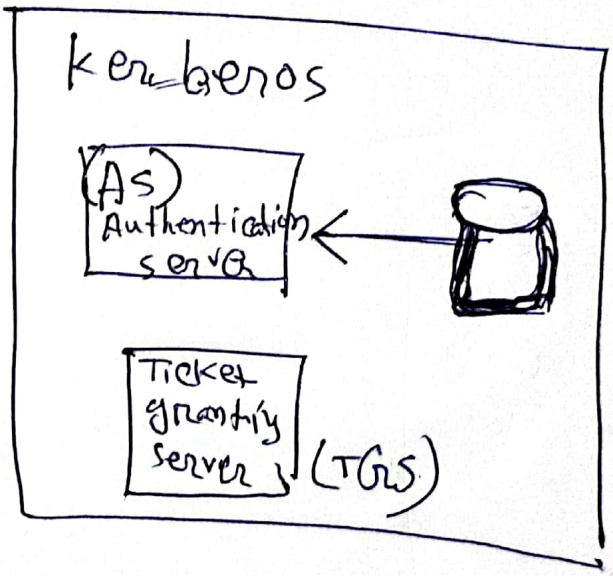
↓

Authentication Algorithm → version 4, 5

MIT — we work with version 4

↓

Authentication সবসময়ই করবে



Encryption করা হয়
যাতে ticket hijacking
না হয়

System থেকে বের হয়ে
নেলে আর service
দেওয়া হবে না,

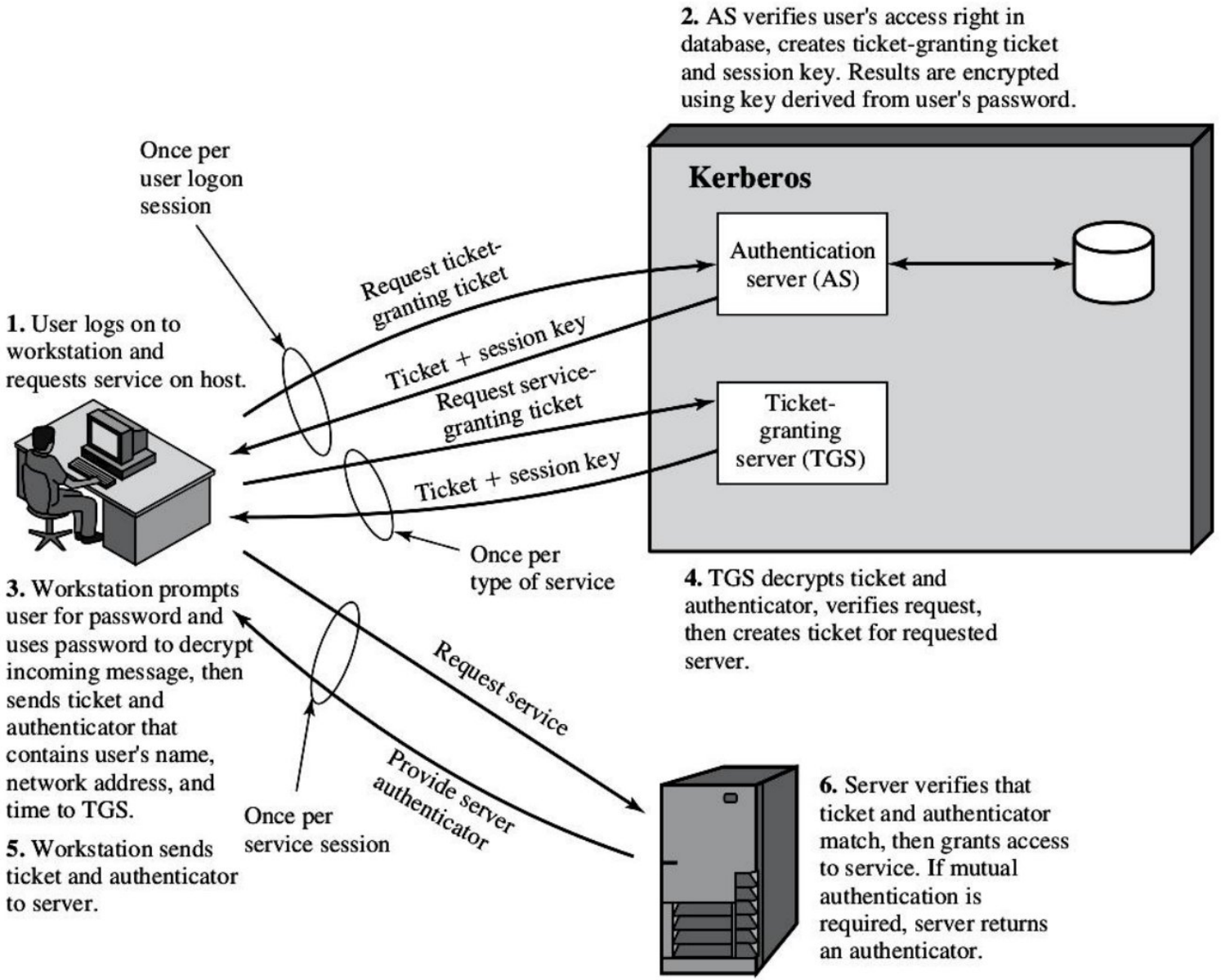


Figure 4.1 Overview of Kerberos

KERBEROS REALMS AND MULTIPLE KERBERI A full-service Kerberos environment consisting of a Kerberos server, a number of clients, and a number of application servers requires the following:

1. The Kerberos server must have the user ID and hashed passwords of all participating users in its database. All users are registered with the Kerberos server.
2. The Kerberos server must share a secret key with each server. All servers are registered with the Kerberos server.

Such an environment is referred to as a **Kerberos realm**. The concept of **realm** can be explained as follows. A Kerberos realm is a set of managed nodes that share the same Kerberos database. The Kerberos database resides on the Kerberos master computer system, which should be kept in a physically secure room. A read-only copy of the Kerberos database might also reside on other Kerberos computer systems. However, all changes to the database must be made on the master computer system. Changing or accessing the contents of a Kerberos database requires the Kerberos master password. A related concept is that of a **Kerberos principal**, which

is a service or user that is known to the Kerberos system. Each Kerberos principal is identified by its principal name. Principal names consist of three parts: a service or user name, an instance name, and a realm name

Networks of clients and servers under different administrative organizations typically constitute different realms. That is, it generally is not practical or does not conform to administrative policy to have users and servers in one administrative domain registered with a Kerberos server elsewhere. However, users in one realm may need access to servers in other realms, and some servers may be willing to provide service to users from other realms, provided that those users are authenticated.

Kerberos provides a mechanism for supporting such interrealm authentication. For two realms to support interrealm authentication, a third requirement is added:

3. The Kerberos server in each interoperating realm shares a secret key with the server in the other realm. The two Kerberos servers are registered with each other.

The scheme requires that the Kerberos server in one realm trust the Kerberos server in the other realm to authenticate its users. Furthermore, the participating servers in the second realm also must be willing to trust the Kerberos server in the first realm.

With these ground rules in place, we can describe the mechanism as follows (Figure 4.2): A user wishing service on a server in another realm needs a ticket for that server. The user's client follows the usual procedures to gain access to the local TGS and then requests a ticket-granting ticket for a remote TGS (TGS in another realm). The client can then apply to the remote TGS for a service-granting ticket for the desired server in the realm of the remote TGS.

The details of the exchanges illustrated in Figure 4.2 are as follows (compare Table 4.1).

that server. The user's client follows the usual procedures to gain access to the local TGS and then requests a ticket-granting ticket for a remote TGS (TGS in another realm). The client can then apply to the remote TGS for a service-granting ticket for the desired server in the realm of the remote TGS.

The details of the exchanges illustrated in Figure 4.2 are as follows (compare Table 4.1).

(1) C → AS: $ID_C \| ID_{tgs} \| TS_1$

(2) AS → C: $E(K_C, [K_{C,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

(3) C → TGS: $ID_{tgsrem} \| Ticket_{tgs} \| Authenticator_C$

(4) TGS → C: $E(K_{C,tgs}, [K_{C,tgsrem} \| ID_{tgsrem} \| TS_4 \| Ticket_{tgsrem}])$

(5) C → TGS_{rem}: $ID_{Vrem} \| Ticket_{tgsrem} \| Authenticator_C$

(6) TGS_{rem} → C: $E(K_{C,tgsrem}, [K_{C,Vrem} \| ID_{Vrem} \| TS_6 \| Ticket_{Vrem}])$

(7) C → V_{rem}: $Ticket_{Vrem} \| Authenticator_C$

The ticket presented to the remote server (V_{rem}) indicates the realm in which the user was originally authenticated. The server chooses whether to honor the remote request.

One problem presented by the foregoing approach is that it does not scale well to many realms. If there are N realms, then there must be $N(N-1)/2$ secure key exchanges so that each Kerberos realm can interoperate with all other Kerberos realms.

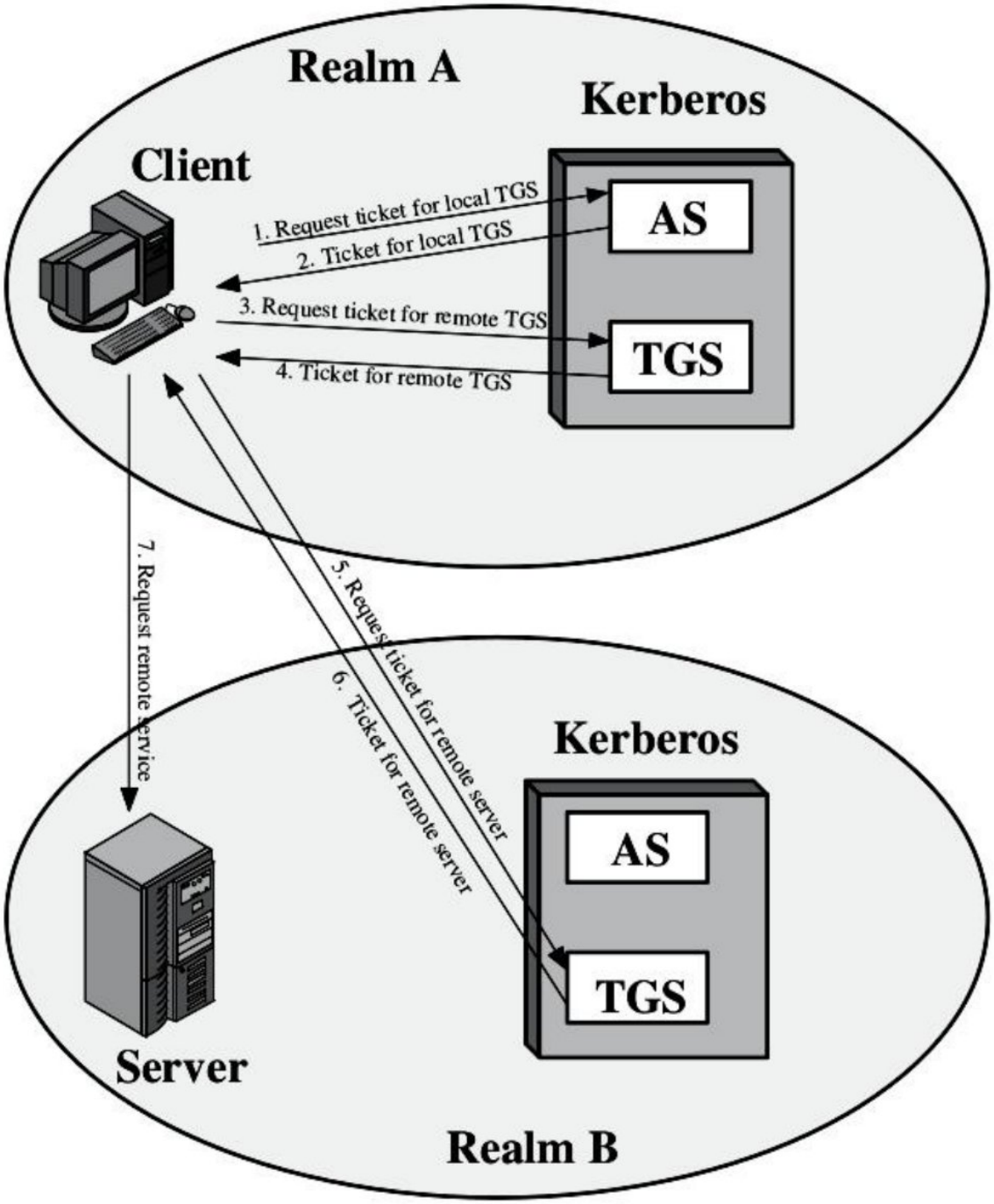


Figure 4.2 Request for Service in Another Realm

Kerberos Version 5

Kerberos version 5 is specified in RFC 4120 and provides a number of improvements over version 4 [KOHL94]. To begin, we provide an overview of the changes from version 4 to version 5 and then look at the version 5 protocol.

DIFFERENCES BETWEEN VERSIONS 4 AND 5 Version 5 is intended to address the

Kerberos Version 5

Kerberos version 5 is specified in RFC 4120 and provides a number of improvements over version 4 [KOHL94]. To begin, we provide an overview of the changes from version 4 to version 5 and then look at the version 5 protocol.

Differences between Versions 4 and 5 Version 5 is intended to address the limitations of version 4 in two areas: environmental shortcomings and technical deficiencies. We briefly summarize the improvements in each area. Kerberos version

4 did not fully address the need to be of general purpose. This led to the following **environmental shortcomings**.

1. **Encryption system dependence:** Version 4 requires the use of DES. Export restriction on DES as well as doubts about the strength of DES were thus of concern. In version 5, ciphertext is tagged with an encryption-type identifier so that any encryption technique may be used. Encryption keys are tagged with a type and a length, allowing the same key to be used in different algorithms and allowing the specification of different variations on a given algorithm.
2. **Internet protocol dependence:** Version 4 requires the use of Internet Protocol (IP) addresses. Other address types, such as the ISO network address, are not accommodated. Version 5 network addresses are tagged with type and length, allowing any network address type to be used.
3. **Message byte ordering:** In version 4, the sender of a message employs a byte ordering of its own choosing and tags the message to indicate least significant byte in lowest address or most significant byte in lowest address. This techniques works but does not follow established conventions. In version 5, all message structures are defined using Abstract Syntax Notation One (ASN.1) and Basic Encoding Rules (BER), which provide an unambiguous byte

restriction on DES as well as doubts about the strength of DES were thus of concern. In version 5, ciphertext is tagged with an encryption-type identifier so that any encryption technique may be used. Encryption keys are tagged with a type and a length, allowing the same key to be used in different algorithms and allowing the specification of different variations on a given algorithm.

2. **Internet protocol dependence:** Version 4 requires the use of Internet Protocol (IP) addresses. Other address types, such as the ISO network address, are not accommodated. Version 5 network addresses are tagged with type and length, allowing any network address type to be used.
3. **Message byte ordering:** In version 4, the sender of a message employs a byte ordering of its own choosing and tags the message to indicate least significant byte in lowest address or most significant byte in lowest address. This techniques works but does not follow established conventions. In version 5, all message structures are defined using Abstract Syntax Notation One (ASN.1) and Basic Encoding Rules (BER), which provide an unambiguous byte ordering.
4. **Ticket lifetime:** Lifetime values in version 4 are encoded in an 8-bit quantity in units of five minutes. Thus, the maximum lifetime that can be expressed is $2^8 \times 5 = 1280$ minutes (a little over 21 hours). This may be inadequate for some applications (e.g., a long-running simulation that requires valid Kerberos credentials throughout execution). In version 5, tickets include an explicit start time and end time, allowing tickets with arbitrary lifetimes.
5. **Authentication forwarding:** Version 4 does not allow credentials issued to one client to be forwarded to some other host and used by some other client. This capability would enable a client to access a server and have that server access another server on behalf of the client. For example, a client issues a request to a print server that then accesses the client's file from a file server, using the client's credentials for access. Version 5 provides this capability.
6. **Interrealm authentication:** In version 4, interoperability among N realms requires on the order of N^2 Kerberos-to-Kerberos relationships, as described earlier. Version 5 supports a method that requires fewer relationships, as described shortly.

Apart from these environmental limitations, there are **technical deficiencies** in the version 4 protocol itself. Most of these deficiencies were documented in [BELL90], and version 5 attempts to address these. The deficiencies are the following.