CSE 490

CIAN A

Cybere – umbrella terem.

Information Assutcance

part → Cybere Security

1. C
2. I
3. A
4. N
5. A

pillars of information assuarcanee

{ Confidentiality, Integricatiy, Availability
Authenticati on, – Nonrcepudiation }

Computere & Cybere almost similare.

CIA triad.

Confidencial → Those who need to know the info

"Need to know"

Encryption Decription → as a key

2 part → Integricatiy → corcrectness of information

Data

Source (name change)

Availability → when the info is necessary then people can access it.

Denial of service attack

Denial of service is against which terms?

Non-repudiation

Neither can deny the way they process the data.

Digital Signature

Authentication → Password

Authentication vs Authorization

5th pillar of info assurance.

comes first

Different from authorization.

username + password (who you are).

Authorization = permissions (what you are allowed to do).

for using → access control

fishing attack.

Risk = likelihood X Impact.

Grandma's computer.

Naval commanders.

Likelihood

→ is a function of threats and vulnerabilities.

→ is an actors that has 2 things →

→ potential and motivation

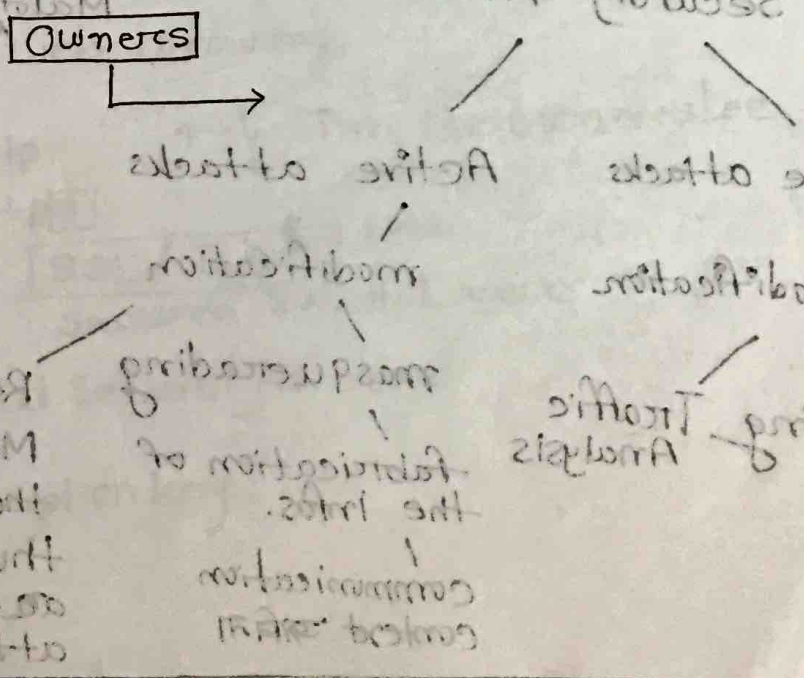
Threat analysis.

Advance Persistant Threat

{ Statistical Analysis
Dynamic Analysis }

Who is a threat to BI government?

Common Criteria Terminologies.



Pen testing / White hat hackers:

Confidentiality : Secrecy & Privacy
privacy assures that individuals control etc influence what information related to them may be collected and stored and by/to whom that may be disclosed.

Privacy - Control of your own information

Anonymity
certain records or transactions not to be attributable to any individual.

Tools
* mixing - Tor browsers } Reddit, Pinterest
* proxies - VPNs
* pseudonyms - fictional identities that can rename real identities.

Will switch

Good → Alice, Bob.
Malorci Bad

Security Attacks.

- Passive attacks
  - No modification
    - Eavesdropping
    - Traffic Analysis
  - No new content added
- Active attacks
  - modification
    - masquerading / fabrication of the infos. / communication context
    - Reply attack: Modify and then reply, thus, forming an active attack.

Passive

Evesdropping — more dangerous.

Traffic analysis.

{Denial of service the interruption or degradation of a data service or info access

Tor browsere
↳ Onion রাউটার কাজ করে

Active Attacks

Alter attack — kind of reply attack
↳ altertation

Denial-of-service

Entity {Either an organization or a person}

Cryptography

Encryption (mathematical function)

plaintext/clear Txt
E (111-22-444).
↓
2AF LE a 22 71005.
↳ Encrypted

Cipher text

Encryption — Digital Signatures

key
↳ Large random number

1. web browsing

Tim Berners Lee

http
https — Lock

SSL / TLS
Secure Socket Layers

Social Security Numbers

Encryption key

plain → cypher

2^{2x} → 8.

(3) key

Infesible

Encryption is a two way function

Hash → one way

Cryptography

Encryption – Symmetric (one key) → shared/secret key

vs

Asymmetric (A pair of key)

public private.

Asymetric encryption; 3 parts.

private – 2 – [3] – 8 public 1

private – 4 – [3] – 64 public 2

Asymmetric

Encryption — confidentiality

Digital Signature — authentication, nonrepudiation

Recipients public key

In assymetric encryption we ~~decrypt~~ encrypt something with receivers public key.

process of elimination.

Senders private key use → Just ~~for~~ using it for encryption

When site signs. Then thecap verify it with his public key if they matche then its verified.

Assymetric Encryption

RSA Algorithm (most famous algorithm).

Turning award.

p q p = 3, q = 11.

n = pq n = 3 * 11 = 33.

x = (p-1) * (q-1) (p-1) * (q-1) = 2 * 10.

relatively prime 20.

Quiz / multiple choice
next wednesday
Tuesday 11

Let's assume that, e = 7.

$(d * e) \% 20 = 1$

③ 7

21 $\% 20 = 1$

public key is $(e, 33) = (7, 33)$ ← product

private key is $(d, 33) = (3, 33)$

RSA key size

Homework

RSA2 Example

RSA slow ← Data Encryption Structure (DES)

AES :faster

AES → better Real time কোনো কিছু করলে cause of speed.

RSA – Symmetrical – দুইভাবে use করা যায়, public & private যদি ৮, উল্টায় দেই then still RSA will work

public key cryp. is summary উপরের গুলোর v. important

RSA
1. Assymetric { Diffi-Hellman ও Symmetric use করা হয় }
2. Slow
3. Both encryption

2nd DS.

Exam question

Diffie Hellman Example

Discrete Logarithmic Principal

Key ~~is~~ always ~~transmit~~ হয়না পাঠানি নেয়নি।

Symmetric Encryption is used in Diffie Hellman
Secret

P = , g assume

P = খুব Large prime number

g = not necessarily prime

P = 7 , g = 2

Alice's secret integer value = a = 4

Bob's " = b = 5.

I) Compute the value that Alice sends to Bob

II) Bob ও Alice

III) secret symmetric key for both

Alice and Bob.

Alice এর নিজস্ব secret

1 That value that Alice sends to Bob,

$A = g^a \bmod P$

mid exam

$= 2^4 \bmod 7 = 16 \bmod 7$

$= 2$ (Ans)

Bob এর নিজস্ব secret

2. Bob sends to Alice, $B = g^b \bmod P$

$= 2^5 \bmod 7$

$= 32 \bmod 7$

$= 4$ (Ans)

Alice $A = B^a \bmod P$

3. Alice sends A to Bob
   Bob sends B to Alice

Symmetric key for Alice $= B^a \bmod P = 4 \bmod 7$

$= 256 \bmod 7 = 4$

Symmetric key for Bob

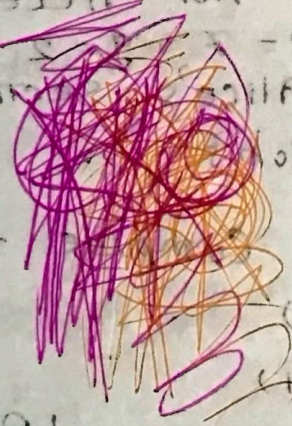
$A^b \bmod p = 32 \bmod 7 = 4$

Quiz

multiple choice.

RSA Digital Signature.

(Lecture 1, 2, 3 > 4 MCQ 5 ?)



$p = 3, q = 11 ; pq = 3 * 11 = 33$

$(p-1)(q-1) = 2 * 10 = 20$

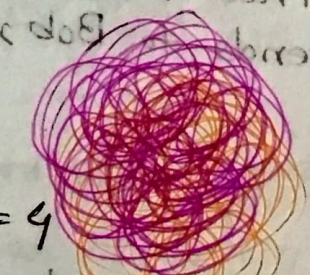
encryption ↳ public key use करते

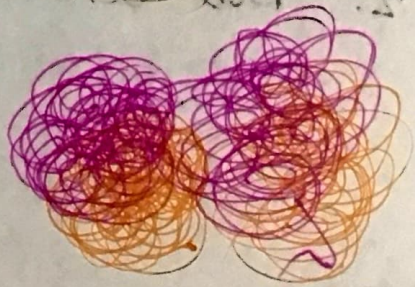
RSA symmetrical

31 is not the encryption version rather it is a signature

(7, 31) going to the receiver verify signature :-

$31^e \bmod 33 = 31^7 \bmod 33 = 4$





Quiz 2 (25/2/24)

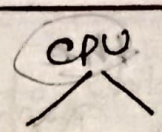
6/2/24

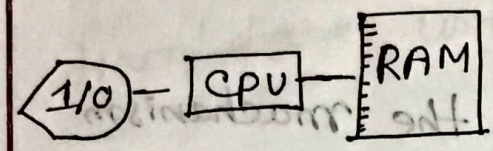
Agenda

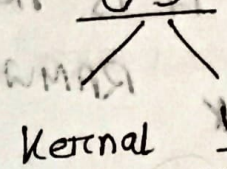
Os review

Os security

Os concepts.







multitasking.

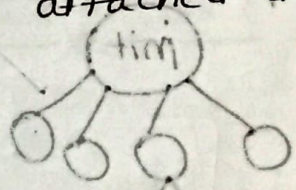
A small slice is given to a RAM

Device drivers.

API - Application Performance Interface

Helps to talk to each other - on an app.

→ most of the cases pc's has the attached device drivers



System calls.

User applications don't communicate with lowlevel or hard drive/ware components and instead delegate such tasks to the kernel, via system call, or syscall for short

(libc) - A collection of programs / library.

r w x

process is the running version of a program

Difference between program and process.

process is very important. when to identify attack it is necessary to findout the process.

RAM

forking

processes are created by the machanism of forking

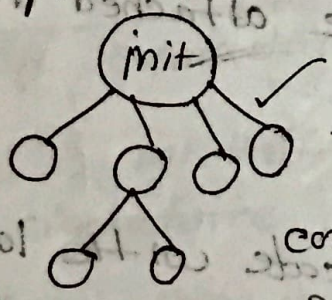
creating new process from an existing process

child. parent

parent ~~PNID~~ init

'init' is the parent of all program

process tree



for

connects

Detecting a malware

process IDs. Users IDs (UID)

PID cpu time memory program Group ID (GID)

Admin user group.

user n n (normal)

process privilege

process security
trusting from parents to child.

Boot sequence.

booting etc bootstrapping.

Hard drive - windows installation

When a

BIOS - (Basic Input / Output System)

Farmware.

BIOS - Operating System

process monitoring.

Password

pass - one way function

Entrophy.

pre computed reverse tracking hash algorithm.

[8] is a good balance for usability and security.

1 sec - 500 combination.

3600 - = 1,80 00000 combination

The attacker needs 2-3 days to try these combinations.

365 / 1800000

Hash has different algorithms.

SHA-1 / SHA-2.

Most of the people use → these algos

password tracking dictionary.

Sony password leak.

privacy is contextual.

[redacted]

26^8 → if we do brute force.

#Dictionary Attack.

worst passwords of 2024,

weakest point - users.

Distributed Denial of Service Attack (DDOS)

Brute force ~~chang~~ checks all possible combinations.

Dictionary all posible combinations.

Random List → Entropy

Textual password আগামী 5 বছরে change হবে না

Rainbow table complicated mathematical opercation

Rainbow table # attack Attacking method,

GPU →

Salt - How to stop the attack

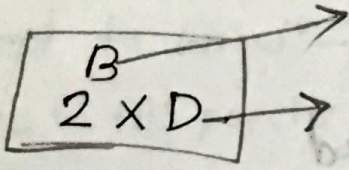
32 bit number randomly নিবো।

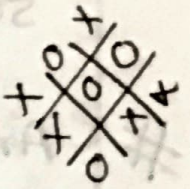
alice - james bond 8475 ttgsawgfh 32bit.

user name salt hash(password + salt)
alice - (james bon + random ------ 32 bit hash)
salt

then hash the full string

resulting hash becomes different.





What is the purpose of password salt?

password salt দিয়ে to prce computed password ~~check~~ attack. get rid of / rainbow table attack.

if two person has same pass but they have different salt so ultimately they are different

client side ২ salt generat হবে then backend ও পাঠিয়ে দিবে।

backend ২ pass-ta কিভাবে থাকে?

Hash & both salt

~~salt~~

#

OS concepts: file systems.

file system - Tree data structure

password - authentication

access control (authorization)

Entity (cyber security)

User
Subject

Data/File
Object

An access control system...

~~print~~ User

permission — read
write

Type

ACE - entry

ACL - List

core 8 principals of cyber security

mount - Add

Windows	Unix
Admin	Root

	User	group	other
	rw_	r_ _	_ _ _

_ file
r read
d directory
w write

file —
directory d

owner	group	others
r w -	r - -	- - -

10 টি placeel option থাকছে } unix এর file configuration

DCO - owner - Read & write
group membership - Faculty.

Not always execute is necessary

Anyone who is not owner are not a person of the group.

"need to know" - যার কাছে কিছু জানানো is not necessary.

State - All parts

Access control matrix / Access control list

	file 1	file 2	file 3
Andy	rx	r	rwo
Betty	rwxo	r	
Charlie	rx	rw	w

matrix rows column matrix

ACLs

Fail-Safe Default

Cybere Security's main rule হচ্ছে Deny যদি permission না থাকে then Deny.

policy | machanism

High level goal → Lower level
→ Do not using calculator

Copying is a pricoblem → Access control করা

High level policy
Low level machanism.

Access control - machanism

append - যা লেখা আছে তার শেষে add হবে।
write - যা আছে সবই overwrite করবে
owner.
copy permission.
copy right
own right.

Instructore	orwca
Lab Instructore	rca
Student.	r

Priciple of Attenuation of Privilage
A subject may not give rights it does not passeses to anothere
নিজের যে permission নেই সেটা অন্যকে কেমনে দেবো
#

(week 6 পর্যন্ত mid এ থাকবে)
Quiz 2 nextweek

ACL is a discretionary → Judgement access control.
(DAC)
Discretionary Access Control.
vs.
Mandatory Access Control (MAC)
→ OS এর যে permission গুলো
→ Implementation Hard.
→ centrally enforcement.

→ আমার pc password আমি control করতেছি।

Important for mid term
Augmented / Extended / Full-blown access control.
IBM's version of the UNIX operating system AIX

Chinese Wall model.
→ From industry
permit, deny, specify

Aug / Full Ex!

AIS.
Augmented Access Control. Next sunday quiz. week 7 বাদ Lecture 12 সমাপ্ত (10, 11, 12)
permit deny specify
specify - precisely permit. (more restricted).
, → (and) logic.
permission - can give new permission
Deny.- অনেক বেশি restricted.
Permit < Specify < Deny
Example for mid: Lecture 12.
base < augmented/extended.
extended এর ক্ষেত্রে base এর conflict হলে always extended follow করবে।
extended always overwrites base.
A Basic ACL wildcard support করেনা। So we need extended.
security design principles → from book.
↓
Implementation এর আগের ধাপ 1975 proposed.
simplicity & restriction. #Bitcoin SHA-2 56 Hashing
keep it simple, stupid.
Economy of mechanism → simple টি choose করা → reusing the libraries.
Fail safe default প্রত্যেকবার check করা

15
86 3
90
1000
1890

eight security design principles.

established encrypted algorithm

SHA-256.

Fail-safe default — connected to Deny

(Default access deny)

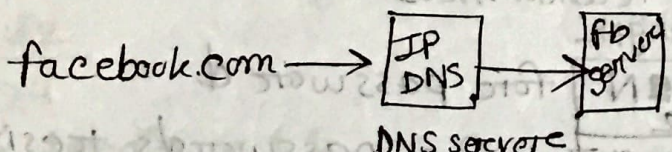
Access control list:

principle of mediation Examples

Text book 2 RAM 2

cash — closest to the hit cache

DNS cash poisoning.



ISP → protect করতে DNS এর motivation আছে।

Secrecy ! = privacy

frequency analysis.

randomization for security

seperation of privilage — A system should not grant permiss based on a single condition

Least privilage

↳ need to know

scalation of privilage. — {password reset, secret answer জানা, know the mail}

Sharing is bad

#

#

Authentication is the binding of an identity to a subject.

Basically of 3 types.

What you know (pass, pin)

What you have (id, physical token)

What you are (biometrics such as fingerprints, voice, eye scan etc)

multifactor authentication - atm card swap.

Entropy

cybersecurity - randomness

$$\text{Entropy} = L * \log_2 N$$ (L → Length) for password

is the measurement of a password's resistence aganist brutte-force attack The formula to compute theorey.

The entropy of tossing a coin $2^1 = 2$

1.

The entropy of cube → 2^2 থেকে 2^3 এর মধ্যে যেকোনো

$4 < 6 < 8$

$6 = 2^x$

$x = \log_2 6$

Entropy = $L * \log_2 N$ → Total no of possible characters in a pass.

L → Length of a password

math

Password min length 6.

Lowercase

Entropy = $6 * \log 26$

$= 6 \times 4.7$

$= 28.2$

uppercase + lowercase.

Entropy, $6 * \log 52$

$= 6 * 5.7$

$= 34.2$

uppercase, lowercase, numbers (26+26+10)

Entropy $6 * \log 62 =$

Min length = 8 (lowercase, uppercase, digit, special char 32)

26
26
10
32
94

$8 * \log 94$

$= 8 * 6.555$

offline → more entropy ↑ more secure

online → user password

Mini length = 11

pass-phrase ↙ password phrase

correct horse battery staple.

$L = 25$ $\quad 25 * \log_2 26 = 25 * 4.7 = 117....$

$\frac{26}{32}$

$\frac{58}{5}$

Jelly+bread ~~101~~ 11 (26+32) $\quad 11 \log 58$

Brcsy**7 lp (6+2) = 8 $\quad = 11 * 5.858$

~~bfa~~ $8 * \log_2 58 =$ → 49.3 bits $\quad = 64.4$ bits

liverpool96 vnwa 77.5 bits.

James Bond 007, $\log_2 62 * 12 = 75.$

4 digit pin

$4 * \log_2 10$ mid-sem syllabus (2 week mid)

$= 13.28$

End sem

~~ea~~ ~~fsh~~ mid excluded
zvx
200. violet → sentence

(3/3/24)

Entrophy

26 * 26 * 26 * 26

effective pass < theoritical pass.

zxcvbn

system generated password

pin 20 - 66
pam 201
CM No. UP 60

2 Factor এ PIN + PASS

Not always PIN as pass cause যে তাদের entrophy 20bit এর কম হওয়া লাগবে।

web pass

60bit এর বেশি অনেক high password.

Solution is hashing.

Using Cryptography to do authentication.

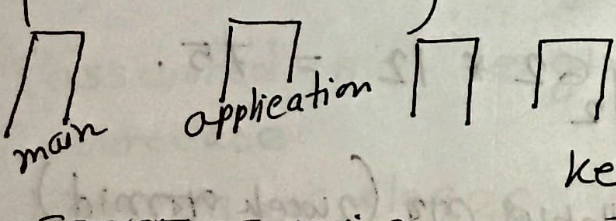
kerberoos authentication protocol.
↓
Why famous →

Server / Desktop

→ Active Directory (Default Authentication Machanism)

→ Greek Mythology → 3 headed animal.

{ Client
Server
Authenticator } → 3 parts.



4টা server
client 100টা

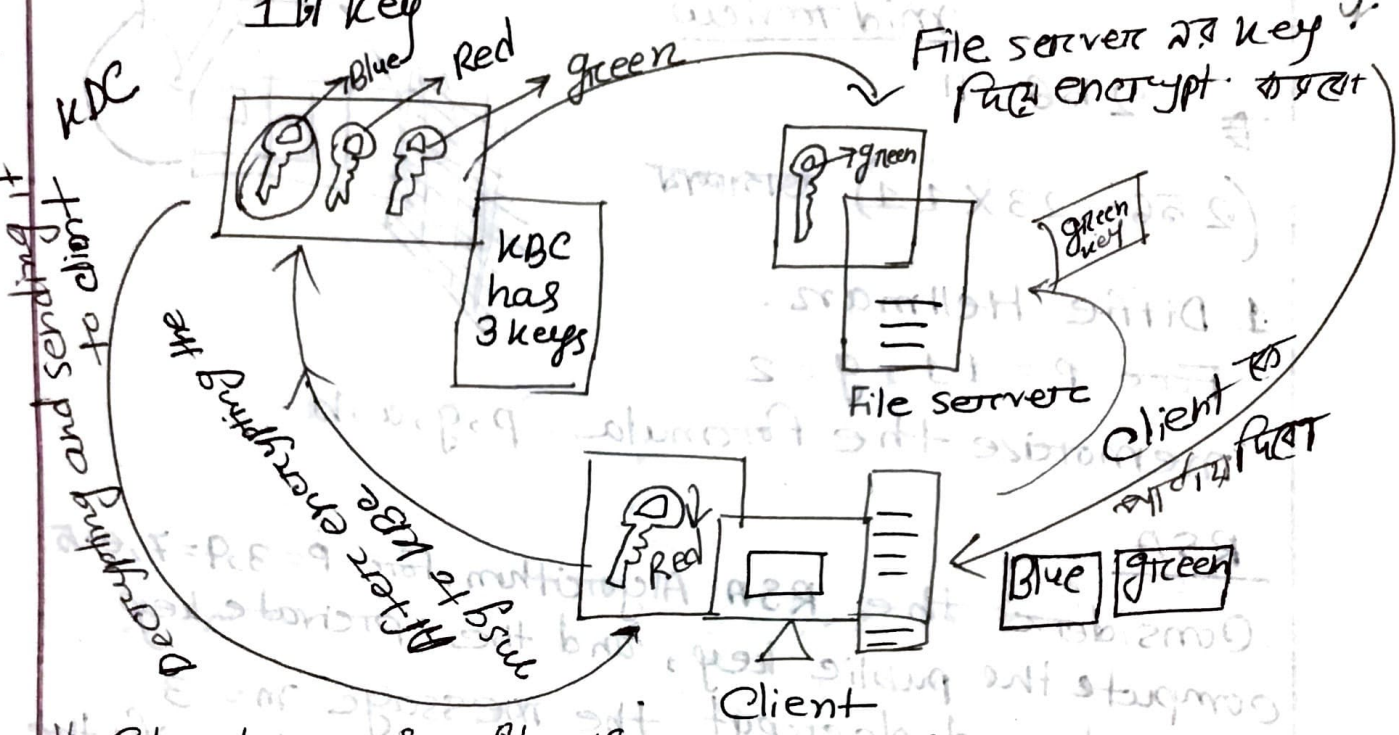
server = service

key distribution center/ Domain controller.

Network authentication

FB নিজের server কে authenticate করতেছে but
এই খানে server কে KBC → authenticate করতেছে।

Cryptography → Difference → Asymmetric → DF Hellman, RS (Imp math) mid
Symmetric → 1টা key



Client proving identity to KBC first
Client encrypting the msg/ticket with his own secret key

Step2

TGT - Ticket Granting Ticket → Blue
Again encrypting with the blue key
Kerbaross → on client's PC

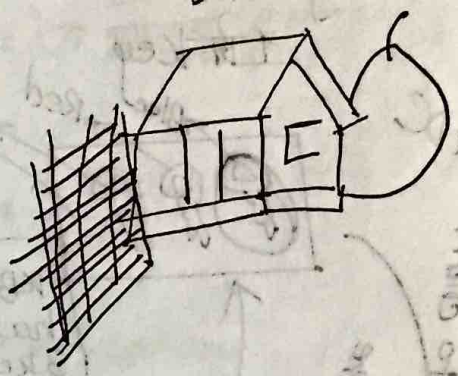
10-12 multiple 10-12
Access control 15
RSA

100 Em - 8টা Secrete
109টা key
Kerbaroos
password transmit হচ্ছে না secret key টা pass হচ্ছে,
HTTPS Public Private এর নাম।
Single point of failure is always risky
keys

mid review

256 ÷ 11

(256 - 23 X 11) ভাগশেষ



1 Diffie Hellman.
For p = 11, g = 2.
memorize the formula. p, g, a, b

RSA
Consider the RSA Algorithm, For p = 3, q = 7, e = 5.
compute the public key, and the private key
Encrypt and decrypt the message m = 3
Sign the message m = 2 and verify the sign
(p-1) * (q-1)
2 * 6 = 12.
(d * e) % 12 = 1 → মুখস্থ
d = 5. 17

$\times \frac{17}{5}$
$\frac{}{85}$

encrypt - public
decrypt - private

Sign করি private
verify public

(e, p*q) public key

msg এর power e public key mod n

$12^5 \bmod 21 = 248832 \bmod 21$

$= 3$

$248832 - 11849 \times 21 = 3$

original plain text wide কর sign এর goal না।

Sign

Signature $2^5 \bmod 21 = 11$.

The value sent was (2, 11).

$11^5 \bmod 21 = 2$.

cryptography - (6-7) marks

→ RSA-, Diffe Hellman

password entrophy

The min length 8.

Atleast one u.c one l.c included After five unsuccessful attempts, the accounts will be locked

Web B → the min length 6. Atleast one U.P, one digit, symbols (!, @, #) n = 5 B.

After 3 unsuccessful attems it will get locked.

→ B offers a better protection Again online attacks because they give.

Locked policy strict - better at online attack.

Entrophy high - better at offline protection

extended permission enable করা থাকলে other permission check করবে otherwise base-ই চলে connection

principle of attenuation of privilage & other permission need to check

2 scenarios check them both.

copy-the permission to give access.

Lecture (1-14) 13marks
12→ marks Lecture notes

16/3/24

1. Cryptographic math/access control/entropy problems 13 marks.
2. Multiple choice questions 12 marks.

R B M O E

ROMBE service attributes

Least privilage
Need to know

Multitenancy

Least common resources should not be shared

Web A = (8) 26+26

$E_A = L * \log_2 N$
$= 45.6$

$E_A > E_B$

$E_B = L * \log_2 N$
$= 6 * \log_2 N$
$= 36.01$

A 5 chances
B 3 chances

B chances < A chances.
B secure

rcw Econom kiss macha
rc Failsafe Deny..
Complete Mediation – every access to every object must be checked for authority
Open - sel = pri
Seperation – two codes one con
Least pr → need to know
Least common me - l
resource sh n

Final Exam

HTTP and SSL

HTTPS (Secure)

Secure Socket Layer/

SSL is the predecessor of TSL

SSL/TLS — They are not much different that's why we write it together

SSL/TLS has two parts

verifying the community

The bank of America

your browser

After successful authentication, symmetric key is used to encrypt the data transmitted.

TLS/SSL Handshaking

The first part → The assymetric cryptography then after the handshaking ends they use symmetric cryptography (Data transmission)

first symmetric
then assymetric

Handshaking begins

Step 1 (Client to Server)

Client - Hey your server

Client hello message

Cipher suites

Your client is sending the things that they support

Step 2 server to client (find the better one)

Step 3 (server to client)

Digital certificate X.509

contains

3. contains servers public encryption key

1 server name

2. The trusted certified Authority (CA)

Step 4 (client) validity trusted X.509.

server's public key

Step 5 (Pre Master secret) based on client server info.

Step 6 (Symmetric Encryption key Generation) Algorithms & math

change cipher — indicating that asymmetric encryption is over and symmetric encryption is about to begin.

initiated by the client/ sent by the client.

Step 8 (Server to Client)

~~paper centred~~

~~people left the chat~~

{Quiz 3 April 2} weeks 7 (24/3/24)

Install software updates + Patch.
#Windows tuesday.
Anti virus are overrated
Software updates are underrated
password manager.
mandatory reading

Usability & deployability needed - textual passwords
expantion - scalable

graphical password
typo loss.
memoriyize effortless না।
Deployability -
= pan accessible
= pan mature & non mature
Passw
Not scalable for user - in ~~biometrics~~ password.
Why passwords will be here for a long time.
usability & deployment

Motivation
user aware last year.

vertical - system এ ঢোকার পর একজনের computer থেকে অন্যজনের computer
lateral - একজনের pc তে

28 তারিখ Final
23 তারিখ Final review

protocol – user friendly হতে হবে।
security is always secondary
But google

2. Abstraction Property
3. Lack of feedback problem (caution feedback).
4. The barndoor property
খোলা রের হলে হলে barrier এর দরজা বন্ধ করে লাভ নেই।

*MCQ The weakest link in cyber security is human/user.
↑
ক. Weakest link
* sphere fishing (Individual target)

30sec - 1min এ user কে কেমনে বুঝাবো। we can't

minimum security with usability.

#properties of a usable system
Learnability
Efficiency
Effectiveness
Error
Memorability

memorability

email pgp - principal of seperation of privilage

Efficiency (Speed in tech).

↳ How long.

Effectiveness (Accuracy).

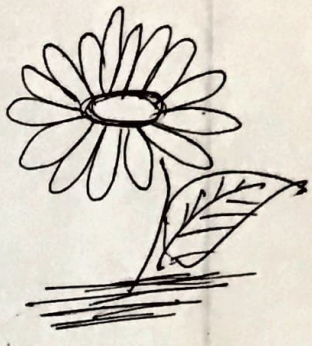
Errors — Dropbox → undo

↳ delete an dangerous error

Immediate user কে কোন feedback দিতে হবে।

Satisfaction/ Engaging

User interface



pretty good privacy (PGP).

Usable security

↳ what to do.

↳ Digital signature, E. দায়িত্ব

↳ public key দিয়ে generate করবো

↳ how to do.

↳ Don't make dangerous error

↳ http/https check করা

↳ suffecientlly comfortable with the interface to continue using it

Security always thinks about threat

Usability " " " threat and victims

both mental model

balance between security & usability

Ecological validity?

↳ Research related to real world