M.J.K. Sir

Goal হচ্ছে এই course এর:-

বিভিন্ন ধরণের security theory আমাকে জানা এবং এইটা হলো Network related হতে হবে।

Security:-

Informal defination:-

(i) Independently ভাবে আমাদ বা প্রয়োজনীয় thing ব্যবহার করা without বাধাবিপত্তি

(ii) Unauthorized access is not allowed

(ii) নম্বরটাকে mainly করা হয় Informal defination of security

Formal:- 3 টা components:-

(i) confidentiality:- আমার personal issue disclose করবোনা আমরা unauthorized person এর কাছে

(ii) Integrity: Data integrity and system intigrity

(iii) Availability: Service এর সময় available হবে Physical structure এর উপর বেশি dependend, logical structure এর উপর কম। authorized user এর কাছে available

Individual, entities, process → 3 টা term আমাদের এগুলো। Privacy is a reason of confidentiality.

Privacy:- নিজের control থাকবে, কাউকে কতটুকু access দিব (এটাকে বলছি degree), কতটুকু information share করবো (এটাও one kind of degree)

(ii)

(a) Data Integrity :- আঘাতের data change এবং destroy হবে না অথবা lost হবে না, কোন একটা unauthorized person এর কাছে অথবা accidental manner.

(b) System Integrity :- system quality এমন ভাবে design করতে হবে যেখানে unauthorized manupulation হবে না।

22-12-2018
1st (E) day

S. S. Sir

→ Cyber security?

Effort যদি Benefit এর চেয়ে বেশি হয় then তা secure
যেমন: RUET এর website টা কেউ hack করতে চাইলে,
তাকে detect করে action ও চলে তারই আগে
হবে, যে hack করতে যাবে।

Bruteforce domain এর search attack টা বাড়ানোর জন্য password এর character বাড়ানো হয়।

Confidentiality : ~~sender~~ Receiver এদেরকে বুঝায়।

Authentication : sender এদেরকে assurance বুঝায়।

Virus : এটা একটা malicious program. এটাকে কখনও software বলবো না। Regular communicati
এ ব্যাঘাত ঘটায়।

Bacteria:- নিজে নিজের replica তৈরী করে। RAM overload করছে।

Logic Bomb : Malicious code এক প্রকার। particular condition satisfy হলে computer ও ছড়িয়ে পড়ে।

Trojan Horse:- (N) Software আকারে install করলে।

Hash Code:- পুরা code এর আগে digest থাকে, পুরা code change করলে digest change হয়। Integrity provide করার জন্যে।

14-12-2018
2nd (B) day

M.J.K. Sir

BOOK- Network Security Essentials
by William stallings (5th Edition)

Chapter: 1

Slide: 3)→ সবকিছুকে artistic representation টা কেমন হতে পারে। respectable way তে আসবে ও যাবে। আমি কিভাবে যাবো, আসবো, departure টা কেমন হবে, তা অবশ্যই artistic way তে হতে হবে। Beautiful, efficient, Power থাকবে artistic way তে। এই way তে যত বেশি কাজে তত acceptable.

Com. Sec. Concepts:-

আমরা যখন data বা information নিয়ে কাজ করবো, কতটা efficient way তে কাজে লাগাবো এবং কতটা Security

provide করতে পারবো। level of parameter এর উপর base করে info. share করি।

এখানে security দুইটা: i) Computer security &
ii) Internet ,,

i) data গুলাকে protect করার এবং hacker এর thwart থেকে রক্ষা করার collection of tools design করা হয়।

ii) ~~data গুলাকে~~ এই measure এখানে transmission of information টা বেশি গুরুত্বপূর্ণ, এটা secured করা, এটা consist হয় measure to deter, prevent, detect and correct security violations. এরব কিছু involve করে transmission of information কে।

Computer security by the NIST:- (slide)

Automated ~~Info~~ Sys:- যেমন: রাত ১২ টার দিকে তেল দরকার গাড়িতে কিন্তু তেল center এ ~~কোন~~ কেউ নাই কিন্তু আমি taka pay করে তেল নিতে পারবো।
এঁর চেহারা
অ্যারের দুর্নীতির উপহরণটা plus Email দিয়ে solve করা

Why we need automated & info. system?
— উপরের কথাগুলো।

Computer security Objectives:-
Confidentiality:- (পূর্বের আগের lecture)
Data conf.: slide.
Privacy:- slide.

Integrity :-

(i) Data Integrity

(ii) System "

Availability :-

CIA TRIAD :-

→ Confidentiality
Integrity
Availability.

Possible additional concept :-

Authenticity :- Uniquely identify করার পর, যে কাজ করে, তাই প্রমাণ করতে হবে, trusted person হয়ে আসতে হবে।

Accountability : Uniquely idetify করতে পারব।

Next day :- → Book
→ syllabus
→ আজকের topic (study).

01-2018
nd (E) day

S. S.
Sir

IP layer, ~~use~~ wireless → Sir topic

IP security :- Internet protocol security ~~হয়~~ Network layer এ। IPV4 এর উপর base করে IP protocol. IP layer এ যেসব security আছে, তাকে বলা হয় IP Sec.

Firewall use করা হয় protection এর জন্য। যেমন RUET gate এর মতো। Windows এর Firewall যেমন।

IP spoofing: ~~আমি mask করলে তার~~ packet যখন pass হয়, Router করে কি Packet ~~data~~ চুনা ~~করে~~ pass ~~করে~~। forward করা। যে কেউ packet টা বানাতে পারে। IP protocol টা আমার known, কিন্তু key টা হচ্ছে unknown। Wrong IP address করে false attacle করা যায়, IP spoofing এর মাধ্যমে total network কে moniton করা যায়। এখন ও IP spoofing করা থেকে রক্ষা করা যায়। এই security provide করা দরকার।

IP security যেভাবে কাজ করে:-
→ Branch office generate করে।

Intranet: একটা প্রতিষ্ঠানের মধ্যে যে network টা local network.

একটা Private IP একটা Public IP. বাইরে access করতে হলে Public Id দরকার। Private IP দিয়ে access করতে পারবো না। যতক্ষণ পর্যন্ত mapping না করছি ততক্ষণ পর্যন্ত access হচ্ছে না বা হবে না। Private IP থেকে বাইরে। Local network এ উদ্দেশ্য হলো, বাইরে যেন access না হয়।

RUET এর semi result এর জন্য Intranet design & maintenance করতে পারি। কিন্তু maintenace করা কঠিন।

থেকে IP security provide করবো। VPN এর মাধ্যমে tunnel তৈরী করে, RUET server কিছু credintial এর মাধ্যমে tunnel তৈরী করবে। Then বাইরে থেকে connect তৈরী করতে পারি। VPN এর মাধ্যমে PC connect হলে ঐ particular Network term and policy এর মধ্যে পরে।

VPN ছাড়াও IP level এও security provide করা যায়। Remote access এর মাধ্যমে করা যায় এটা।

☐ At least 40 টা malicious program এর Name + কাজের বর্ণনা। (Assignment)

5-01-2019
3rd (B) day

M. J. K.
Sir

Network security & Adatures

OSI Security Architecture

- i) Security Attack
- ii) Security Mechanism
- iii) Security Service

~~Thread~~

(i) এটা এমন এক ধরণের action যেটা compromise করে security of information, owned by a company.

Security পড়ার উদ্দেশ্য হলো যে, কোথায় আমরা এটা apply করতে

(ii) একটা process যেটা design করা হয়েছে, যাতে করে security attack detect করতে পারি, এবং এটা কিভাবে recover বা ~~Recover~~ Prevent করবো security attack থেকে।

(iii) এটা হচ্ছে একটা communication service যেটা enhance করে data processing system এর security এবং একটা organization এর info. transfer.

Threat :- একটা threat হচ্ছে একটা possible danger যেটা might exploit (কাজে লাগানো) a vulnerability (ফাকফোকর)।

A potential for a violation of security, এটা exist করে যখন কিছু action security টাকে breach করে এবং harm cause করে

Attack :- পড়ে নিতে হবে slide.

Security attack :-

Active attack :- An active attack attempts to alter system resources or affect their operation.

Passive attack :- Does not affect system resources.

Fig: 1.1 (slide)

Passive attack 2 প্রকার :-

Traffic analysis : এটার মাধ্যমে জানতে পারি, কে কার সাথে কত দ্রুত communicate করে।

আরেকটা প্রকার : slide, &

Goal : slide.

Active attack :-

Masquerade :- এটা ঘটে যখন one entity pretends to be different entity.

Replay :- বার বার একি জিনিস পাঠানো।

Modification of Msg : কিছু portion update করা হবে, record করা হবে।

Denial of service : Management service provide করতে চাইলে বাধা দিবে।

Active attack এর goal হলো attack কে detect করে এবং recover করে যে কোন ধরনের ~~dist~~ disruption থেকে

Goal এর আগের দুইটা প্যারা slide.

Security service :-

Defined by X.800 as :- এরা কিছু service provide করে by a protocol layer of communicating open system

অর্থাৎ এটা ensure করে ঐ system এর যথেষ্ট security.

Defined by RFC 4949 as:-

একটা communication service যেটা একটা system provide করে, যাতে করে একটা specific kind of protection দিতে পারে ঐ system resource এর।

Service category (slide)

Table (1.2) (slide)

Authentication:- (X.800)

Peer entity auth.: ঠিক person এর আসলেই কথা বলছি এটা ensure করাই।

Data origin auth.: ডাটা টা ঠিক জায়গা থেকে origin হচ্ছে কি না, তা ensure করে।

Access control: কিছু ability যেটা limit বা control করবে host system এর access service টা access করার জন্য identification দিতে হবে।

Data confidentiality:-

The protection of transmitted data from passive attack

The protection of traffic flow analysis.

Data integrity :-

connection oriented, connection less (আগের ধাপ)

NOn Repudiation :-

এটা prevent করবে, যেন একটা message কখনও deny হবে না যদি sender ও Reciever যথেষ্ট identified হয়।

Availability :- (1st page এই দাগর)

Availability service :-

- এটা ensure করে availability
- এটা depend করে proper management and a control of a system.

Table 1.3 (security Mechanism)

Model of Network security :- (Fig: 1.2)

- Slide.

Network access security Model :-

Opponent হতে পারে human, software

Fig (1.3) → Slide.

Unwanted Access :- Slide.

Program can present two kind of threats :-

Info. Access threat : একজনের কথা আরেকজনকে বলা যেভাবে বলছে তার কোন data তার access নাই।

Service threat :- যারা যে service টা চাচ্ছে সেটা পাচ্ছে না, বা যেটা পাচ্ছে সেটা চাচ্ছে না

NIST → একটা society

(i) National Institute of Standard and Technology.

Last point → slide

(ii) ~~NIST~~

ISOC → একটা society.

(i) Internet security

Last point → slide.

29-01-2019
4th (B) day

আগের class এ যা পড়াইলাম,

Beach of security level → slide

Two types of Passive attack → »

X.800 → slide.

RFC. 4949 → slide

Model of Network Security → »

স্যারের পড়াশুনা (2nd slide)

Plaintext, ciphertext etc → slide.

Fig 2.1 → "

Symmetric & Antisymmetric ---

Brute Force attack → সব possible attack check করতে time অনেক বেশি লাগে তাহলে।

Feistel encryption & decryption (16 round)

* 16 টা round কেন?

Reasonable time লাগছে, hacker কে hack করতে অনেক বছর লাগবে, আর সেই বছর ঘুলার পর msg ঘুলার value কমে যায়।

→ কয়েক যুগ.

Feistel cipher design element :-

Block size, key size, ---- → slide.

Symmetric block Encryption Algo :-

Three most important symmetric block cipher :-

(i) DES (ii) AES (iii) 3DES

DES → Data Encryption Standard

AES → Advanced " "

3DES → Triple Data " "

Block cipher :-

Process করবে plaintext কে ciphertext এ।

DES Algo :-

Slide.

The strength of DES :- Slide.

Triple DES :-

Guideline of 3 DES :-

AES Encryption & Decryption :-

RANDOM & PSEUdo random Numbers :-

~~Kerberos~~ :-

Replay attack → বার বার একই msg send করাই।

Randomness :-

(i) Uniform distribution :-

(ii) Independency :-

Fig 2.6 → Random, Pseudorandom number generatons.

Algo. design :- Next day পড়বা।

Fig 2.7 → Stream cipher Diagram.

$Mss = E(Ms, ks)$ ⟶ Encryption

$MS = D(Mss, Ds)$ ⟶ De

Stream cipher design considerations:-

RC4 algo :-

Fig 2.8 → RC4

Cipher block modes of Opt :-

Electronic codebook mode:-

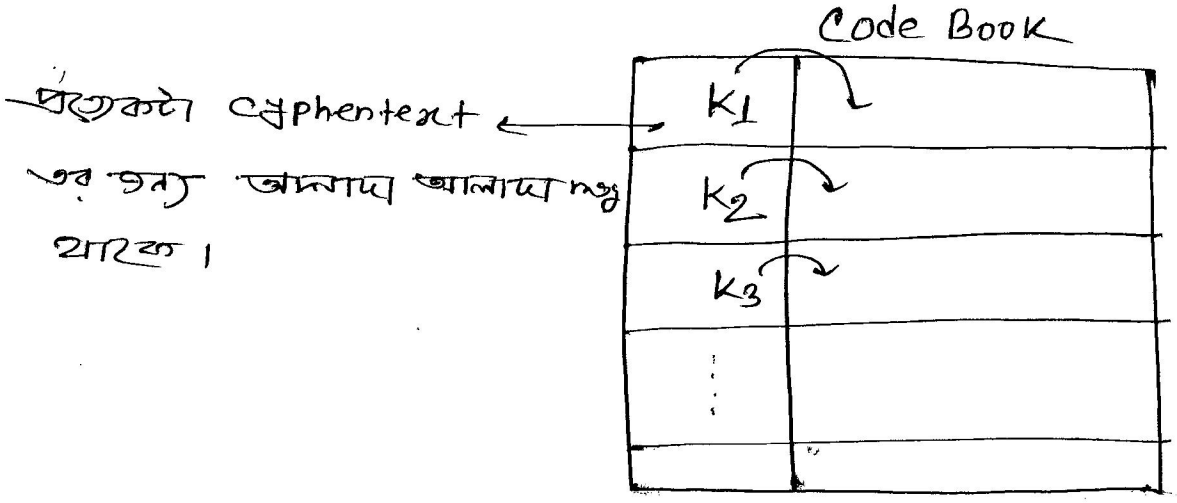


Fig 2.9 → Cipher Block Chaining (CBC) Mode.

Fig 2.10, Fig 2.11

Adv. of CTR →

12-02-2019
4th (d) day

S. S. Sir

IP Security:- Network administrator, vendor (3rd party) provide করা।
Application ~~সুরক্ষা কোথায়~~।

Router → একটা Network কে আরেকটা Network কে connect করে। Routing process টা হয় Network layer এ থাকে। Network device কাজ করে Network layer এ। ⊠ , , এর সাথে IPSec

করে।

IP Sec কি ?

Ans:-

① Secure branch office:- Completely security provide করে। IP Sec provide ~~করে~~ করে VPN এর মাধ্যমে।

② Remote login :-

③ Electroic commence security :-

④ Intranet & Extranet :- provide করে Network layer এ এই check টা হয়।

IP Sec এর benefit :-

(i) Network layer এ provide করা হয়, যারা vendor আছে তারাই এটা ensure করে যে আছে তাদের IP Sec আছে। Vendor group user এর interaction ছাড়াই router তৈরী করতে পারে।

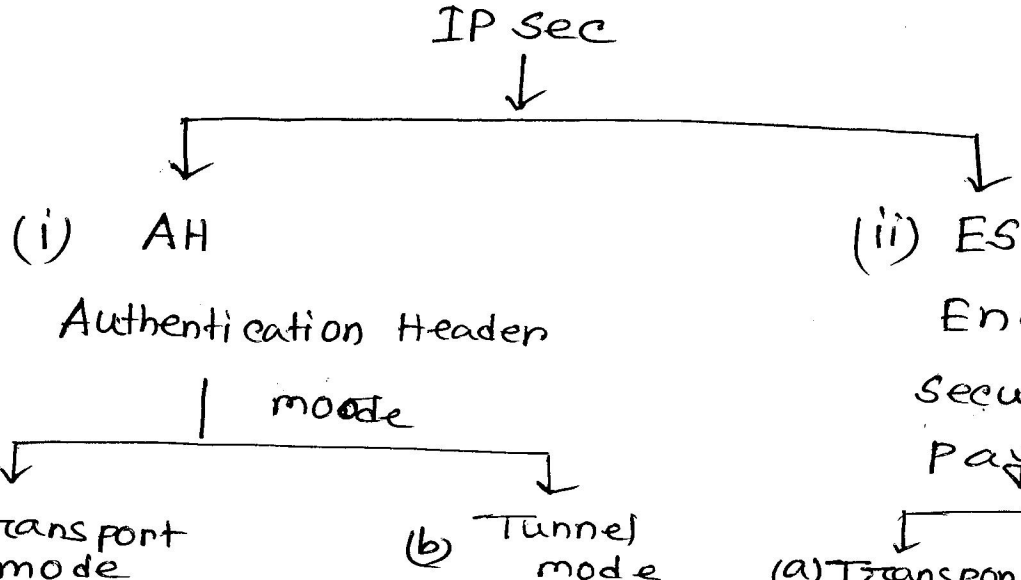
(ii) Organigation এর employee গুলোকে train করার প্রয়োজন হয় না। User কে train করার ঝামেলা নাই।

(iii) Security কে bypass করার কোন way নাই।

(iv) IP Sec provide করে Firewall তৈরী করতে।

Any info router থেকেই বাইরে ~~থাকবে~~ যাবে এবং ভেতরে আসবে so Router এ IPSec থাকলে এটা strong security provide করে।

IP sec. এর আরো দুইটা protocol:-



(i) Authentication ও Integrity provide করে।

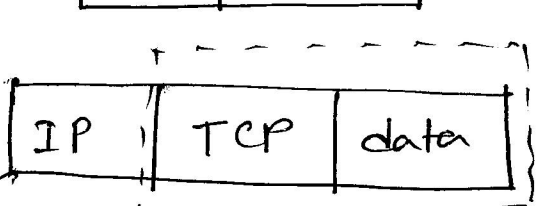
(ii) ,, (optional), Encapsulate করবে msg টাকে, Confidentialy provide করে

Data link ও layer ও ডাটা থাকে। Transport layer ও ডাটার আগে header add হয়। layer গুলার কাজ আগের ধাপে।

→ Transport layer

প্রত্যেকটা layer ও এরকম করে header add হয়

Network layer ও IPsec protocol যুক্ত হয়।



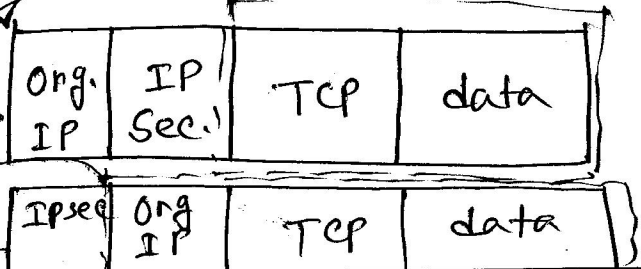
→ Network layer

→ এটা Transport layer ও কাজে লাগে।

Org IP header টা open

TCP ও data এর উপর security provide করে।

Org IP, TCP, data এর উপর



Transport mode.

Tunnel mode

Tunnel mode ও org IP header তা open না। ওখানে encript করছি ও authentication দিচ্ছি org IP, TCP ও data এর উপর।

05-02-2019
5th (B) day

Chap-03

M.J.K. Sir

- Approaches to message authentication
- Secure hash functions (SHA)
- Digital signature (DSA)
- Message authentication code (HMAC)
- Public key cryptography principales
- " " " Algo. (RSA)

NS1 → Slide → Slide Name,

Need for security :-

Slide.

An Intro. to cryptography :-

Passive বা active attack ও আমি বুঝতে পারি না যে, ও intruder listen বা alter করছে msg টাকে।

Slide.

Transposition cipher :- (syllabus এ নাই)

Symmetric key Algo:

Public key Encryption (RSA) → Slide

SHA → Slide.

SST, TLS → Slide.

Freedom of Speech :-

Possibly banned material :- 68 NO Slide.

Steganography : 69 Slide.

Slide Name → ~~Net~~ Ch03 NetSec 5e

Approaches to Message Authentication :-

i) Using conventional encryption

ii) Without message "

i) একটা key দ্বারা encrypt

" " " decrypt

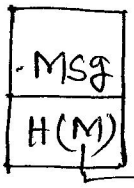
Fig 3.1 (MAC)

→ এখানে msg টাকে encrypt করছি না যা msg আছে তাই থাকবে।

ONE way Hash function :-

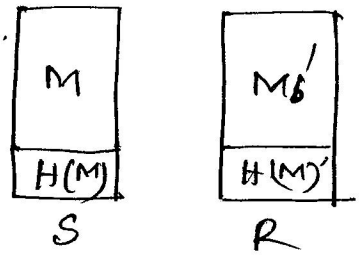
→ what is Hash function?

বর্ণনা Slide.



→ Challenging হচ্ছে H(M) টা authentic কিনা

Fig: 3.2 Message Authentication Using one way hash funct



$H(M) = H(M')$ → Alter হয় নি Msg ট

$H(M) \neq H(M')$ → " " Msg ট

Secure HASH Functions:-

→ যে কোন block of data এর উপর H apply করলাম

→ H টা produce করবে fixed length output

→ H টা এভাবে হতে হবে

↓

বাকিটা slide.

Security of HASH Functions:-

Cryptanalysis:-

Brutefonce attack:-

09-02-2019
5th(d)day

S. S.
Sir

IP Sec service:-

(i) Access ~~Action~~ control

(ii) Connection less integrity

(iii) Data origin Authentication

(iv) Confidentiality.

(i) এটা particular কোন file এর উপর হবে না এটা, যদি করি এটা হল category হবে IP address এর উপর base করে। R এলাকার Router কে স্থাপন করবো,

local private addreess এর উপর base করে IPsec use কর[illegible]
পারে।

(ii) Connectionless ও কোন dedicated কোন Path থাকেনা। ~~[illegible]~~
~~[illegible]~~ IP address সহ pack করলে।

(iii)

(iv) ENcapsulation Security payload provide করে এটা।

Security association:-

One way relation from sender to receiver. এর জন্য[illegible]
assocoiation থাকবে। One way relation from receiv[illegible]
to sender । এর জন্য একটা association থাকবে।
এদের 3 টা parameter থাকে:-
i) SPI (Security parameter Index):-
i) IP destination Address:-
i) Security protocol Identifier:-

→ তুলা থাকে

~~SPD:~~ SPD: Security Policy database. প্রত্যেক Router[illegible]
এর সাথে connect, যে Rout[illegible]
এ IP sec টা Implement হয়[illegible]

SA (Security Association) selector:-

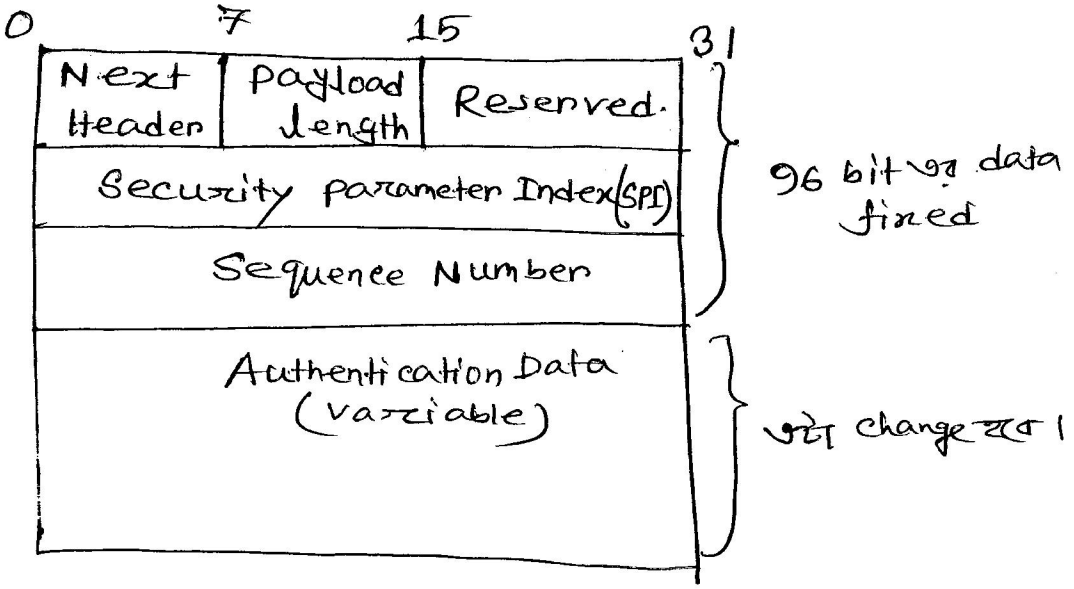
একটা IP add এর জন্য একাধিক Association থাকতে পারে

একটা Asso[illegible] এর জন্য এক[illegible] IP add. থাকতে পারে

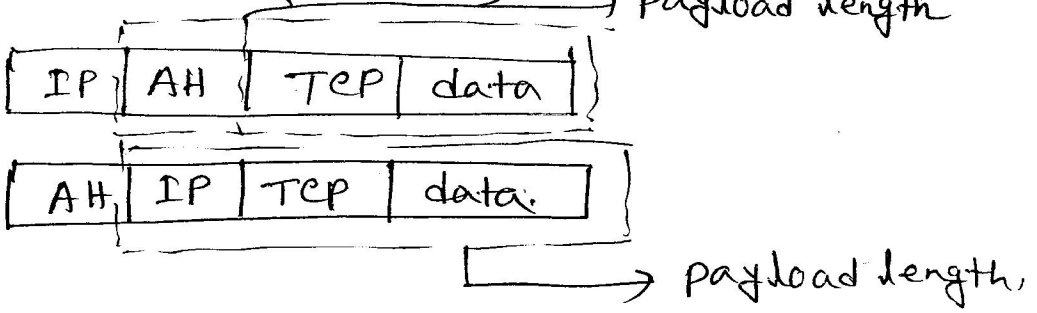
DES → পড়বো।

Block Cipher, 16, 32 bit এর হতে
পারে।

H- Header দেখতে এমন:-



Orginal Header যেটা ছিল,



Reserved: future এ use এর জন্য।

SPI: Header পৌঁছে এখন Index Number টা দিয়ে SPD এর সাথে link করবে, then communication করবে।

Sequence Number:- ~~Duplicate~~ Replay attack থেকে বাঁচায়। 2^{32} no. use করতে পারে। এটা Enble করা হলে, 1, 1 করে বাড়তে বাড়তে 2^{32} পূর্ণ হলে, নতুন security association তৈরী হয়।

Authentication data:- 96 bit এর মধ্যে প্রতিস্থাপন করা হয়। Hash এর first or last ~~bit~~ 96 bit এখানে থাকে। sender ও Receiver

১২৮ এ তার মত প্রকাশ করে ~~ওখানে~~ যে ~~কখন~~ কোন bit রাখবে। log…
96 bit এখানে রাখে।

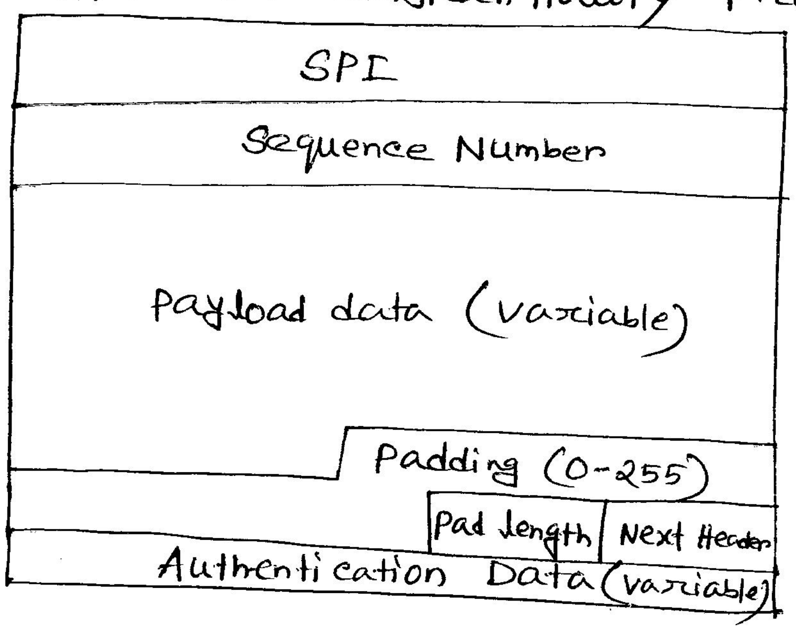
Hash : Fixed length data produce করে।

MD-5

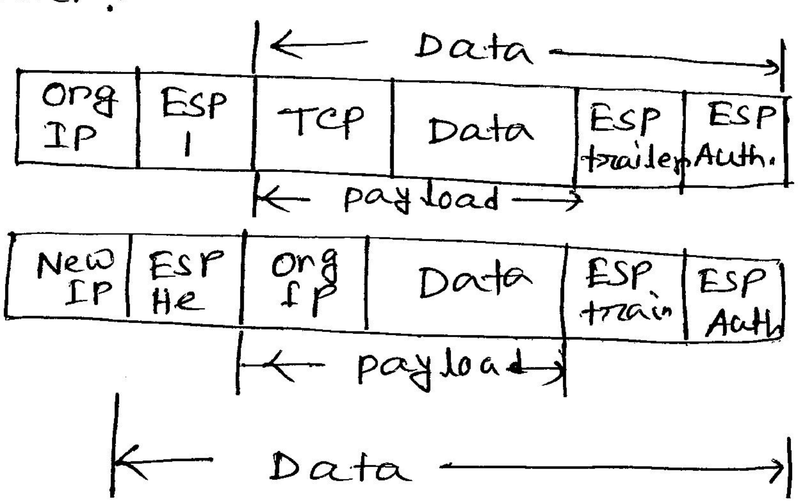
SHA-1, SHA-2 --- SHA-3

HMAC → use করে SHA-1

ESP-Header :- Encription টা বাধ্যতামূলক, ওখানে বাধ্যতামূলক না। এটা Confidentiality provide করে ESP-protocol use করলে IP-sec…



Original Header :-



Transport mode

Tunnel mode (total টা Encription হয়)

SPI → আগের টায় মত

Sequence NO → " " "

Padding → এখানে DES use করা হয়। Round off করার জন্য use করা হয়। Pad length এর মাধ্যমে gap টা খুঁজে বের করে।

Authentication data → আরো

23-02-2019
6th(B)day

M.J.K. Sir.

Approaches :-

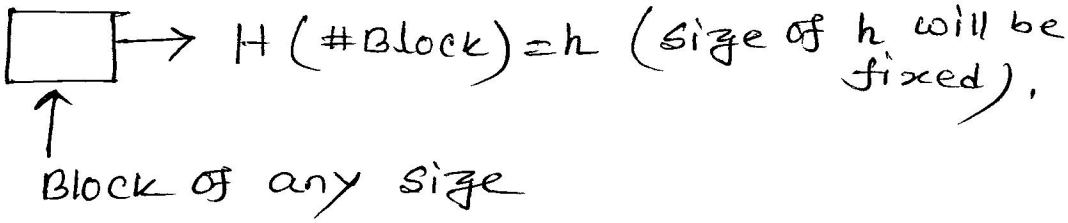
→ Using conventional encryption
→ Without Encryption.
→ RSA

The SHA secure HASH Function :-
└→ Secure Hash Algo.

Comparison of SHA parameter :-

Fig: 3.4 SHA-512

Secure hash functions :-



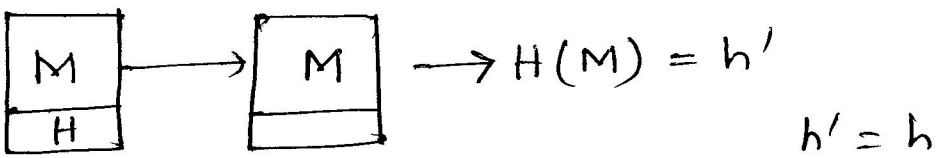
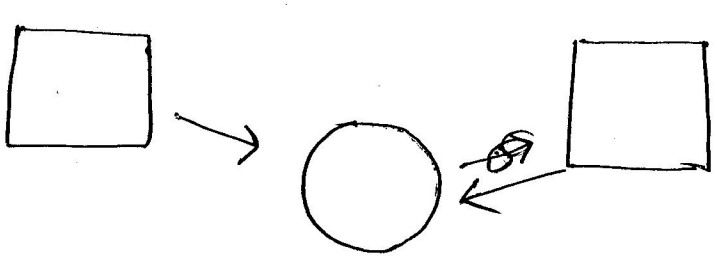


Fig: 3.5 → Slide.

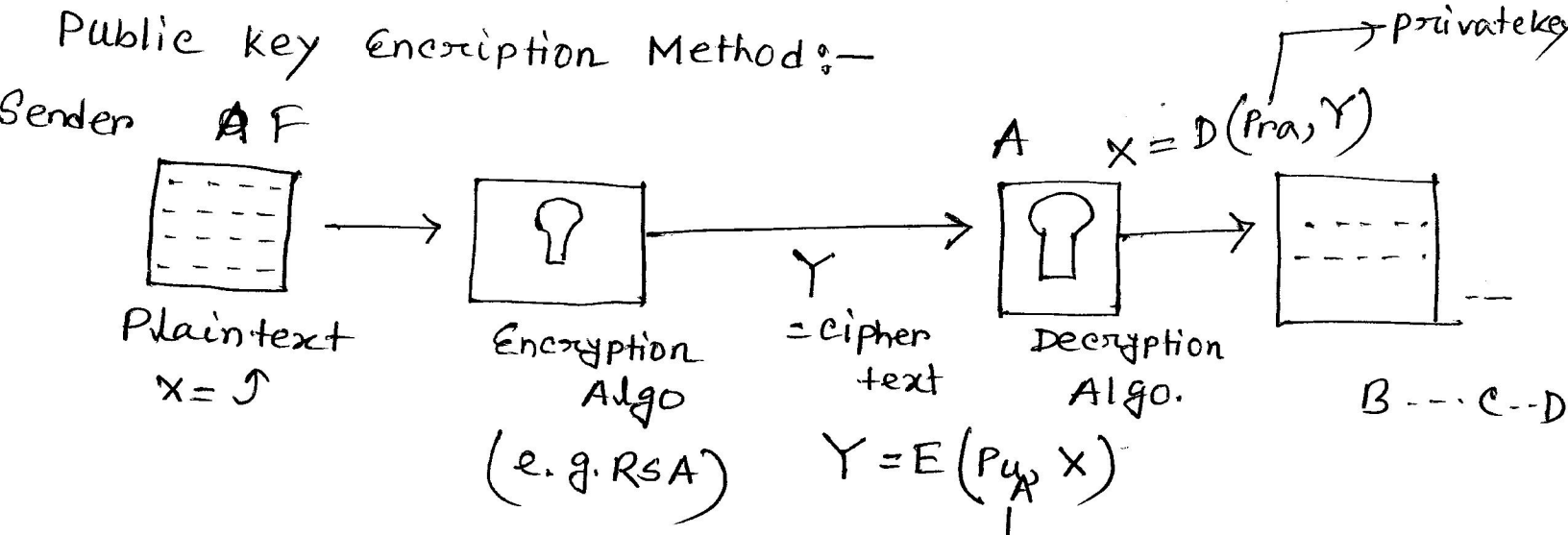
SHA-3



HMAC

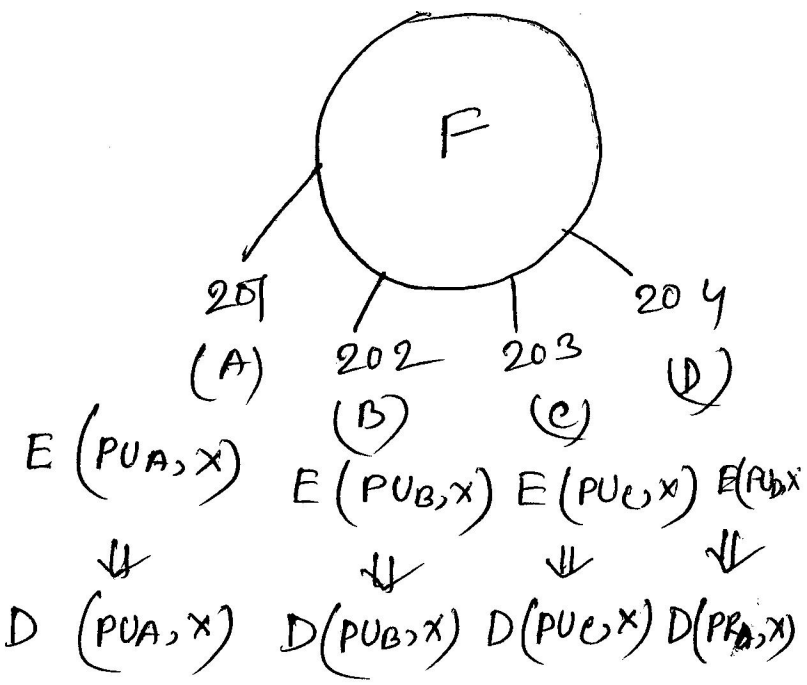
↳ Hash Message Authentication code.

Public key Encription Method :-



Deffihellman Algo :-

Slide No. 23



Public key En. Tech. → En/Dec
→ Digital signature
→ Key Exchange.

-02-2019
5th(d) day

S. S.
Sir

Web security

Application layer ও কাজ করে।

WWW (World wide web) একটা distributed system. এই system কে চালানোর জন্য http, etc থাকে। Fundamental communition হয় server ↔ client, এখানে যত security হয় সব provide করে web security. Web security টা provide হয় transp layer এর আওতায়।

Server ↔ client ও security impose টা challenging. online ও communication টা হলো two way Comm এক্ষেত্রে খুবই challenging কাজ হল security impo করা two way communication এর ক্ষেত্রে।

Web page, we use করা, design করা easy, এর underline tech. টা extremely complex, এখানে কোন idea না থাকলে। এখানে হচ্ছে layer of abstraction, এখানে web security provide করা challenging.

Business এর security drop করলে business টা মুহূর্তের মধ্যে ধ্বংস হবে! ~~কোন কারণে~~ এখেত্রে challenging. Two way stone.

Web user রা maximum untrained. এক্ষেত্রে challenging.

অতএব, web security provide করা challenging.

17-02-19
7th(B)day

M.J.K.
Sir

One way Hash function:-

$D = H(M)$
↓ ⟵ Variable sit
Fixed size

The secure Hash function:-

MD-4

Public key cryptosystem:-

Fig 3.9: public key cryptography.

Application for public key crypto System:-

(i) TLS
(ii) SSL
(iii) STL

06-03-19
8th(B)day

M. J. K. Sir

NS1 → Slide.

Need for security.

P = 73 e = 27

M1 1001001 = 73

P1 1010010 = 82

C = M1 ⊕ P1 = 0011011 = 27

P2 = 1011110 =

C ⊕ P2 = 1000101 =

Quantam cryptography :-

Symmetric key Algorithm :-

কেন দরকার পড়লো Advanced encryption standard

» আমরা AES কে use করছি DES (Data Encription Standard) এর জায়গায় ?

DES
- → Block size বেশি হওয়ার কারণে slow
- → 46 – 48 ঘন্টার মধ্যে Encript করা possible decrypt
  - → parallel computer use করে

→ record করিয়ে 16 থেকে 10 এ আনা হয়

DES AES.

Cryptanalysis :-

13-03-19
9th (B) day

Nahid Sir

Verilog / VHDL

↳ Detail Electronics design করা হয়।

Board viva

High Level Language.

↓

Compiler

↓

Assembly Language

↓

Assembler

↓

Machine Language

↓

Instruction Set Architecture — Connect Point between Hardware and software.

↓

Computer Architecture

↓

Digital Electronics

↓

Analog Electronics

↓

Transistor.

RISC, CISC এর পার্থক্য? কোনটা ভালো?

4-bit Computer design:

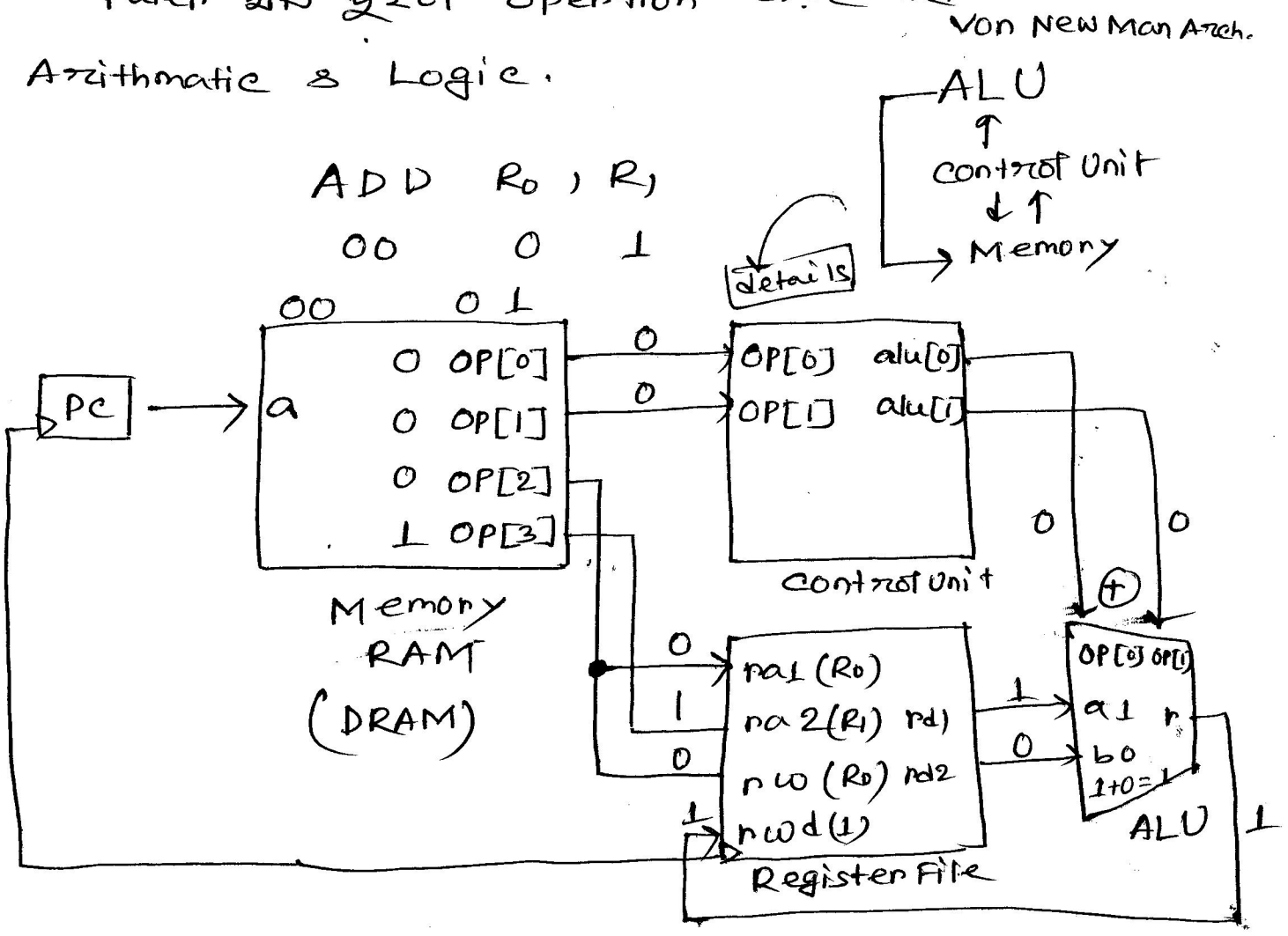
Opcode	Operand 1	Operand 2
2 bit	1 bit	1 bit
ADD 00	0/1	0/1
SUB 01	0/1	0/1
AND 10	0/1	0/1
OR 11	0/1	0/1

Register Instruction

Computer এর দুইটা operation করতে পারে

Arithmatic & Logic.

Von New Man Arch.



ADD R0, R1

00 0 1

R0 = R0 + R1

ধরে নিই,

	Before	After
R0 এর মিত	1	1
R1 , ,	0	0

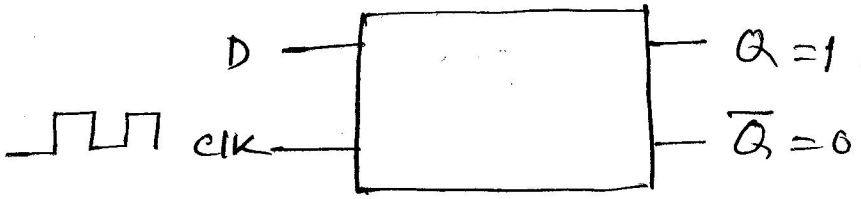
RAM ⟶ SRAM, DRAM ⟶ capacitor (Refresh করতে হয় তাই ছোট)

⟶ Flipflop (Refresh করতে হয় না, তাই বড়)

⟶ Bit ধারণ করে

SRAM faster but cost এর কারণে DRAM use করি।

Register এর মিত Flip flop আছে।



D Flipflop

এ value টা ধরে রাখবে Next clock cycle পর্যন্ত।

Combinational circuit ⟶ Instantaneous

Sequential " ⟶

Clock define করে, তাকে gate defing করে, Next clock cycle

Clock এর কাজ হল instruction গুলো যেন sequential perform হয়। তাই Processor এর guard বা পাহারাদার হিসেবে কাজ করে।

13-03-2019
9th(B)day

M.J.K.Sir

Ch04 Net Sec5e

→ Slide.

S: 8/9/10/11 → H.W

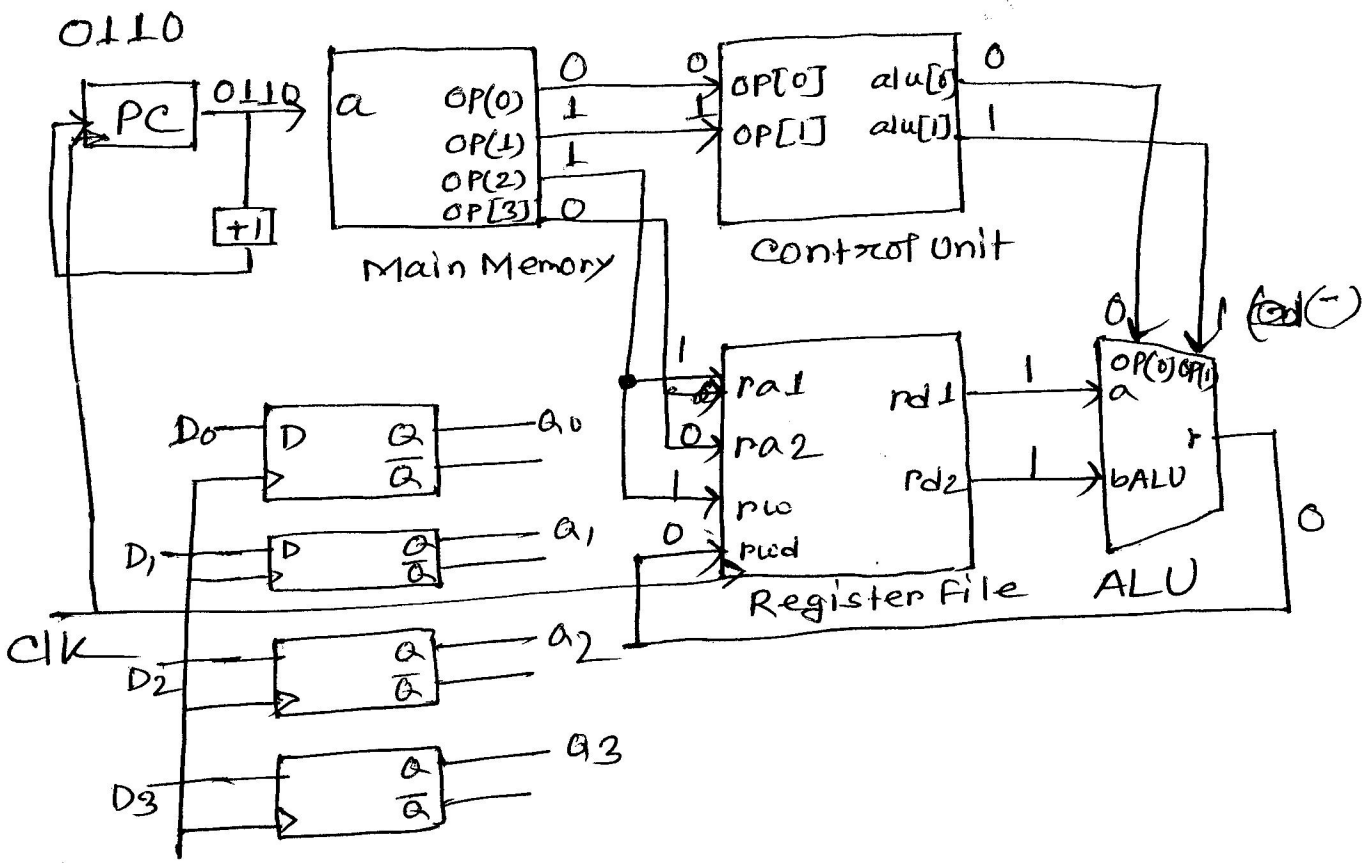
12/13

18-03-2019
9th(D)day

Nahin sir

4 bit Computer

Opcode	Operand1	Operand2
2bit	1bit	1bit
ADD 00	0/1	0/1
SUB 01	0/1	0/1
AND 10	0/1	0/1
OR 11	0/1	0/1



OP[0]	OP[1]	alu[0]	alu[1]
0	0	0	0
0	1	0	1
1	0	1	0
1	1	1	1

$$alu[0] = OP[0] \cdot \overline{OP[1]} + OP[0] \cdot OP[1]$$

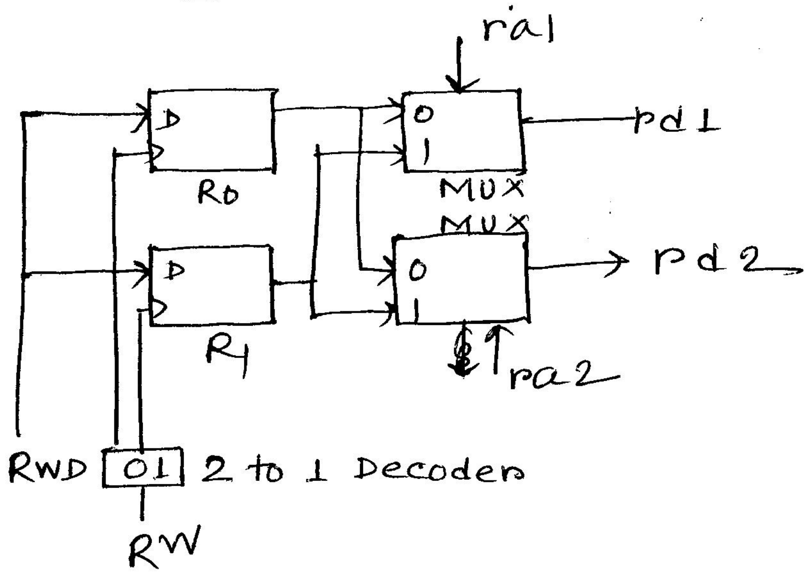
$$= OP[0] \left(\overline{OP[1]} + OP[1] \right)$$

$$= OP[0]$$

File.

Javascript Engine

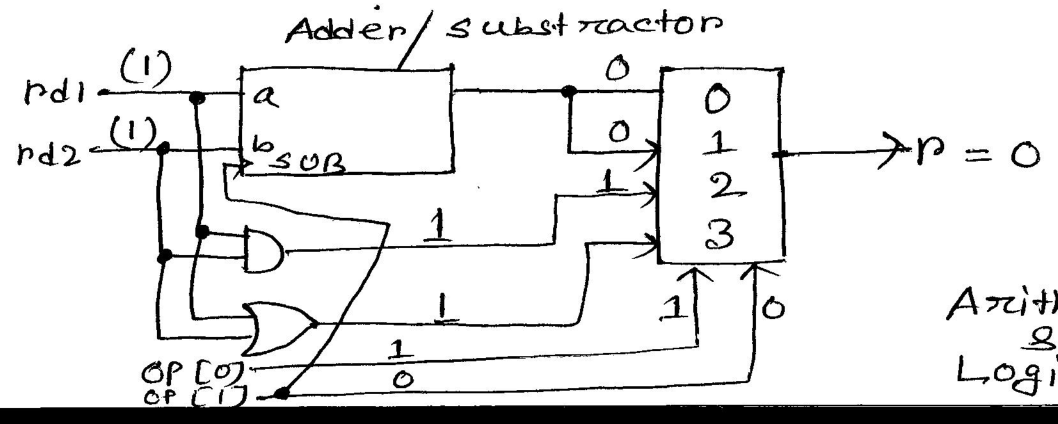
Register design টা দেখতে কেমন ?



ALU design টা দেখাও ?

0 = ADD

1 = SUB

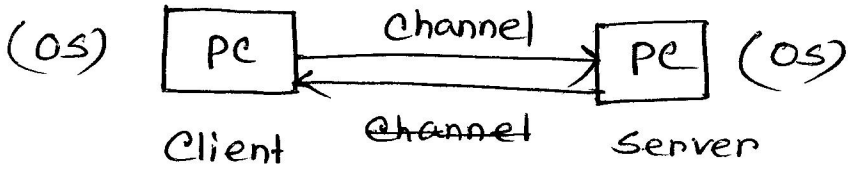


Arithmetic & Logic Unit.

1-03-2019
10th (B) day

Web Security

Nahin sir



Computer security :-

System software (OS) - কে রক্ষিত (protect) করা বা secure করা।

Network security :-

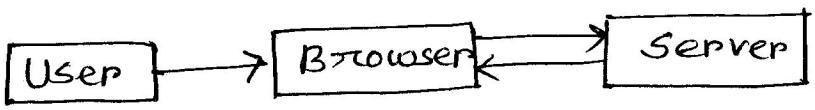
Communication channel টাকে secure করা।

Cyber security :- CS + NS

System security :- For particular organization এর security ensure করার জন্য।

16.1

Web security considerations :-



Web browser এ অনেক component আছে এবং complex অবস্থায় আছে। complex software এটা। এখানে explore করা অহেতু।

Server protect না করলে অব important info ফাঁস হবে এবং company এর loss হবে।

User :-

User ও security provide করা possible না. আগের দুইটার ক্ষেত্রে " " " possible.

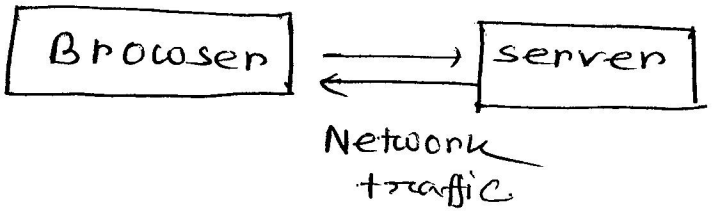
Web security Threats :-

One way → Passive Attack (যাকে attack করবে সে বুঝতে পারবে না)
One way → Active "

Passive Attack → Evasdropping
Passive Attack → Access to restricted info.

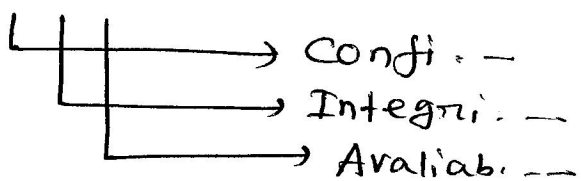
Active Attack → Impersonation (আর একজনের user Name দিয়ে)
Active Attack → Modification (Info টা modify করলে).

Another way



আমরা এইটা consider করবো সব সময়।

CIA



	Threats	Consequences	Counter measures
Integrity.	Modification by virus, trojen horse, logic bomb	Loss of info	Cryptographic checksum Hash → MAC

logic bomb: অনেকগুলা condition আছে, কোন একটা condition satisfy করলে active হবে logic bomb.

~~Trojen horse~~:

MAC → Message Authentication Code.

↳ → Message এর integrity check করা।

Message এর আগে code add করবে।

code দিয়ে varify হবে।

Integrity ensure এর জন্য MAC ব্যবহার।

Encription → privacy ensure করা।

Integrity , করে MAC.

	Threats	consequences	Counter Measur
Confidentiality.	Evasdropping theft	Loss of privacy	Encryption

	Threats	Consequences	Counter Measure
Denial of services / Availability	Flooding Machine with useless request	Disruptive Annoying	Difficult to prevent.

↳ ~~ইচ্ছাকৃত request পাঠানো~~

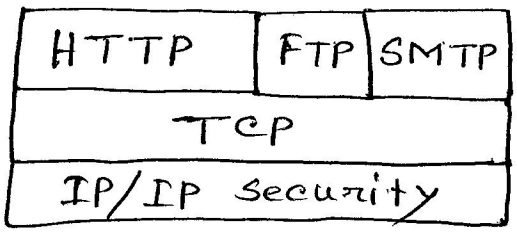
	Threats	Consequences	Counter Measure
Authentication	Impersonation	Misrepresenation of user.	~~Certificate~~ Cryptographic Techniques.

Https ~~এ~~ অবস্থায় password ~~দিলে~~ Evasdrop ~~করতে~~ পারে।
Secure ~~করা~~ যায় না।

Https ~~এর~~ Opposite.

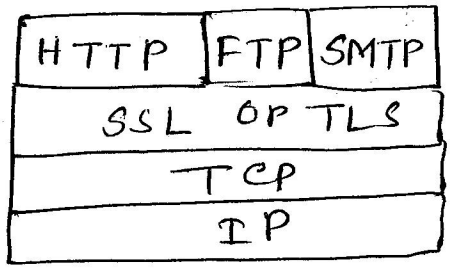
Web security Approaches :-

(a)



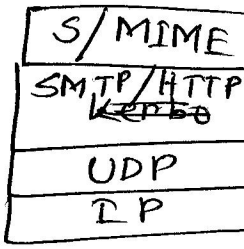
(a) Network level.

(b)



(b) Transport level

(c)

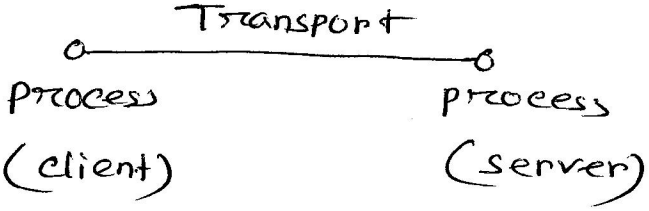


(c) Applicati level.

↳ Secure.

S/SMTP → Simple Mail Transfer protocol
MIME → Multipurpose Internet Mail Extension.

Transport এর ছোঁয়ে,



24-03-2019
10th (B) day

M. J. K. sir

Ch04 Net-Sec - Key Distribution

08-13 no slide (Home Work)

AES (Home Work)

→ code টা implement করতে হবে।

11th (B) day তে এটা submission.

Fig: 4.2

Kerberos Exchange.

আমাদের দিন: Threads & Attack.

-03-2019
10th (D) day

SSL

Con. → Encription

Ava. → Difficult → বাদ দিয়ে বাকি তিনটা provide করবে SSL

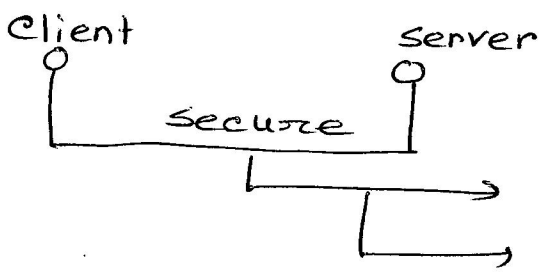
Int. → MAC

Au. → Digital certificate

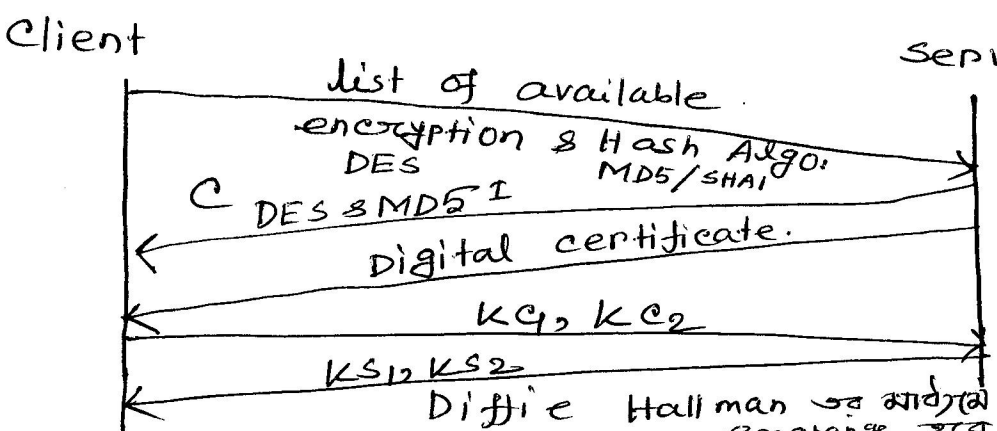
HTTPS

SSL এর new version টা হচ্ছে TLS, বর্তমান আমরা যেটা ব্যবহার করি সেটা TLS.

SSL/TLS uses TCP to provide reliable and secure connection between Browser (client) & web server.



এটা করে Handshaking এর মাধ্যমে।



DES এর মাধ্যমে Con. provide করা ও MD5 Int. provide করে Digital Cer. Au. provide করে।

~~Pu~~

Public key private key

$E(Pu, M)$ $D(Pr, E(Pu, M)) = M$

একজন যার কাছে private key আছে সেই decrypt করতে পারবে।

CA (certification Authority) :-

(CPr, (server name, server public))

→ এটা private key দিয়ে encrypt করবে।

Public " " decrypt " ।

D (CPu, E (CPr, (server name, server public))

= (server name, server public)

~~এটার মাধ্যমে~~ certification authority র Public key দ্বারা decrypt সম্ভব। এটার মাধ্যমে Authentication provide করা সম্ভব।

= 0 =

client server

DESc use করে KC_1, DESs use করে KS_1, KC_1

$KC_1, KS_1 \rightarrow DES_c \rightleftarrows DES_s \leftarrow KS_1, KC_1$

$KC_2, KS_2 \rightarrow MAC_c \rightleftarrows MAC_s \leftarrow KS_2, KC_2$

HTTPS establish করতে আগে SSL provide করতে হবে
তাই আগে SSL provide করলাম।

16.2 SSL & TLS

~~SSL record protocol~~

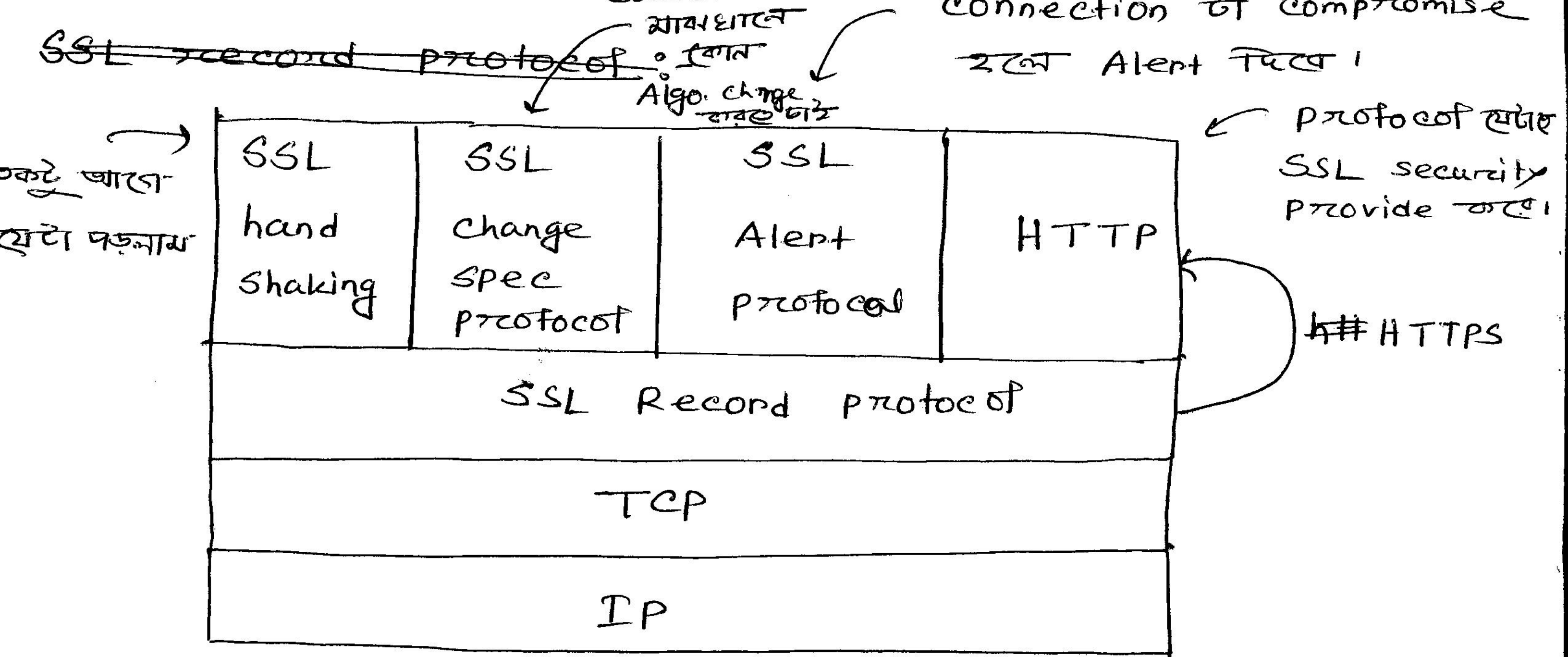


Fig: SSL protocol stack.

① Connection (data transfer এর জন্য)

② Session (Client এবং server handshaking এর মাধ্যমে intial connection তৈরী করে).

Session state	Connection state
1. session Identifier.	1. Server & client random
2. peer certificate.	2. Server write MAC secret key (ks2)
3. Compression Method.	2. Client " " " (kc2)
4. Cipher spec. (DES+MD5).	3. server write key (ks1)
5. Master secret key.	4. client " " (kc1)
6. Is resumable	5. Initialization vector
	6. Sequence Number.

Block Cipher use করা হয় block এর উপর। এখেত্রে use করি mode of Operation use করি। এখানে লাগে Initialization vector.

01-04-2019
11th (B) day

Nahin Sir

CTF:-

Capture ~~the~~ The Flag.

→ এটা হচ্ছে server এর information.

Website:

hackerone.com (এই website ও hacker করা হয়)

→ অনেক tutorial আছে hacking করার জন্য।

Penitration testing (কোন System এর দূর্বলতা খুঁজে বের করে).

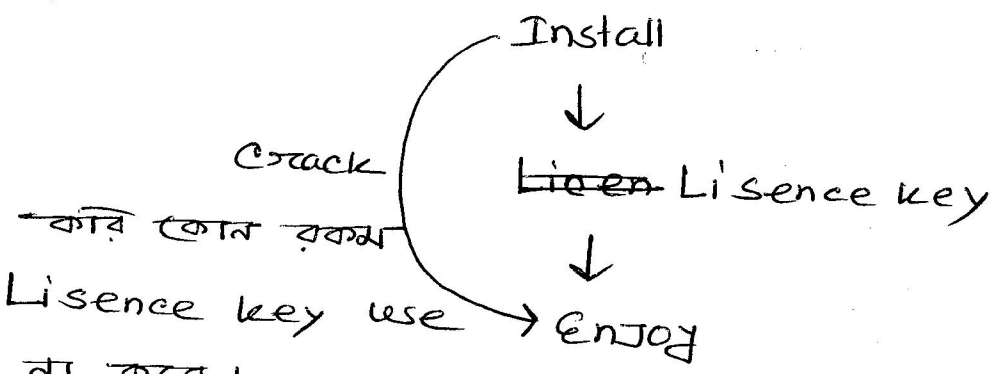
White hat hacking → কোম্পানির ভালোর জন্য hacking (Ethical hacking).

Red " " → ক্ষতি করার জন্য

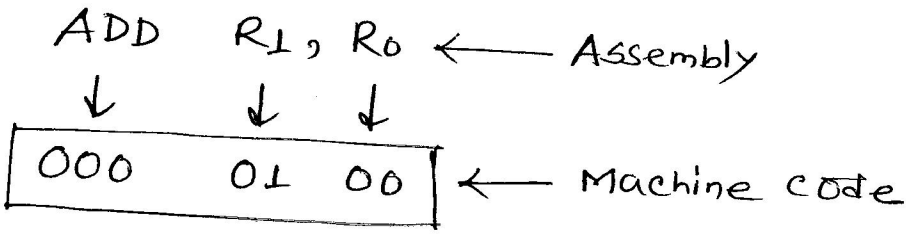
Crack:-

Full feature use করবো, কোন রকম টাকা পয়সা না দিয়ে করবো আমরা cracking.

এখন একটা flow chart দেখি:-



Assembly এর আগে machine code এর অর্থ কি?



এরা direct source code টা দিয়ে দেয় Machine code এ পরে Disassembler use করে Assembly টা পায় পরে hacker রা অহতে access পায়। ফলে Lisence key টা আর দরকার হয় না। এই full process হলো Reverse Engineering (কোন system break করাই)

তাহলে কোন software Reverse engineering করে অহতে break করা অসম্ভব।

Soln:-

Unnecessary machine code করে দিবো, ফলে Reverse Engineering টা কঠিন হয়, একে বলা হয় software obsfucation. 100% software Reverse engineering বন্ধ করা possible না।

VIRUS টা কিভাবে attack করে তা জানবো software reverse Engineering এর মাধ্যমে।

DSP course এর এর কিছু ~~হয়~~ use হয় mp3 তে।
Open source codecs হলো একটা mpeg.

SSL Record protocol :-

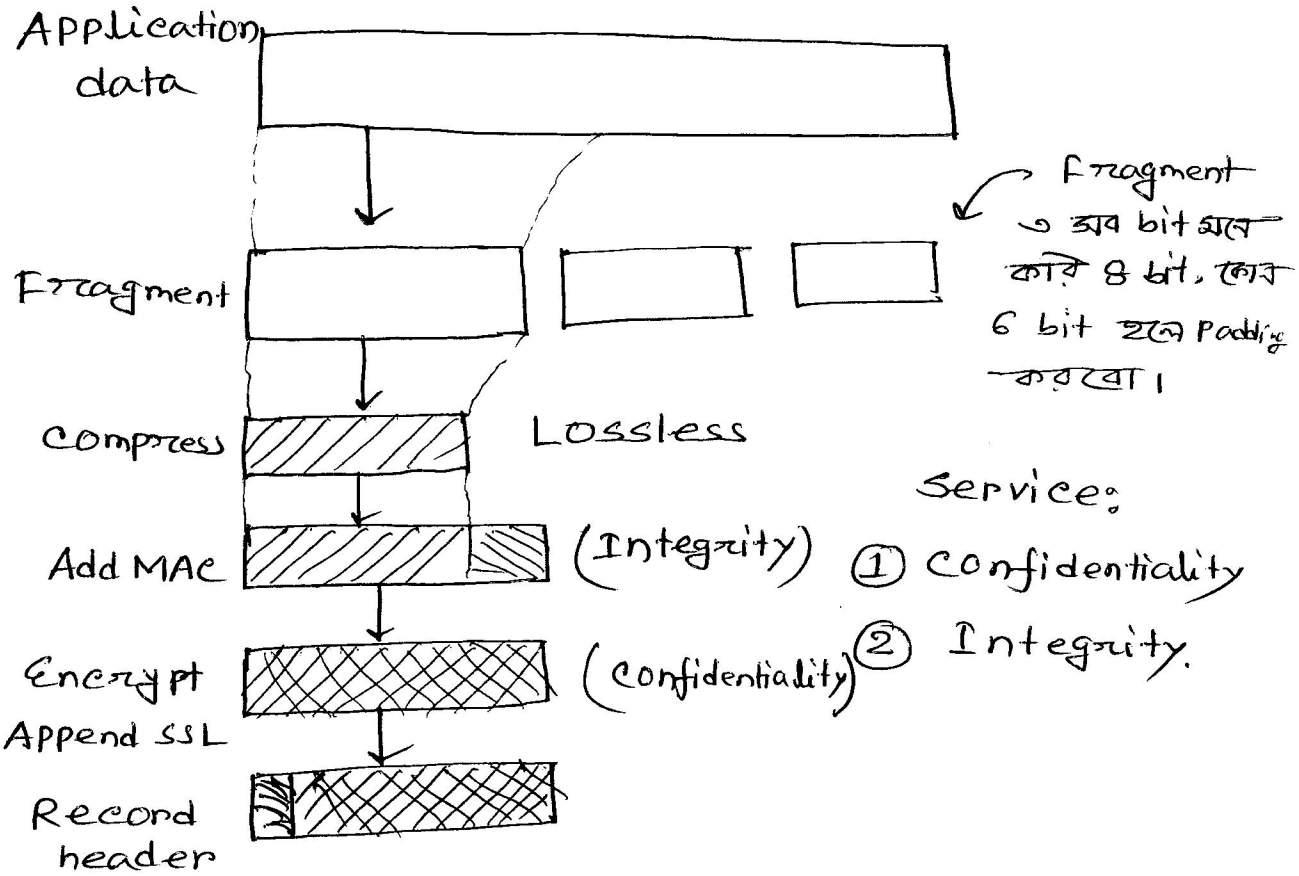


Fig: SSL Record protocol operation

Algo: (ADD MAC)

hash (MAC_write_secret || pad_2 ||

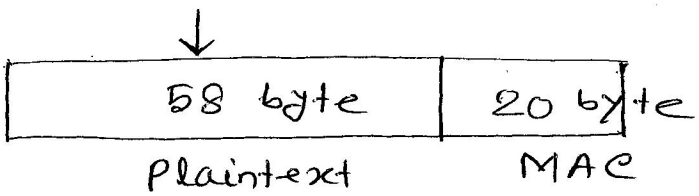
hash (MAC_write_secret || pad_1 || seq_num ||

SSLCompressed.type ||

SSLCompressed.length ||

SSLCompressed.fragment

))



$58 + 20 = 78$

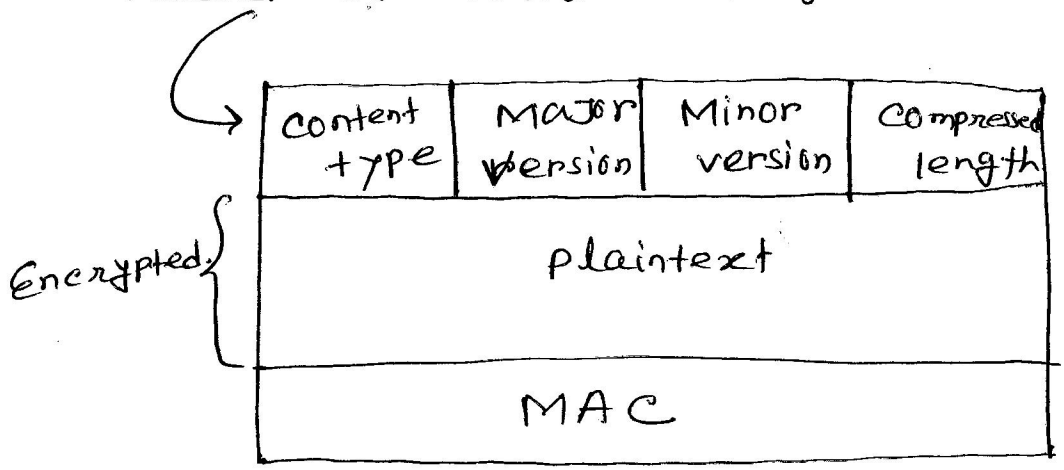
প্রত্যেক pad করতে চাচ্ছি 8 bit করে ফলে,

$78 + 2 = 80$ ✓ $\quad 80/8 = 10$

Padding + padding byte + length padding
1 ① fixed

length padding টা অব অবশ্য 1 bit fixed.

~~hear~~ header ও total view :-



SSL Change spec protocol :-

MD5 initialize করছি, তখন মনে করছি তার জায়গায় SHA-1 use করবো; আগে NO compression ও জায়গায় compression. কোন কিছু change করতে এটা use হয়। এটার size হচ্ছে 1 byte এই 1 byte এর ভিতর অব code থাকে, এই code

টাই define করে কি কি change করে।

Next day → Handshaking

03-04-2019
11th(D)day

Bayezid sir

Slide class

Fig: Handshake protocol

08-04-2019
12th(B)day

Wireless security → অ্যার পরে পড়াবে।

Adhoc wireless Network:-

Fixed কোন rule নেই। অর্থাৎ কোন অবস্থাকে instant/ immediately চালনা করা। কোন fixed communication থাকে না।

AdHoc কেন wireless ও use করা হয়?

↳ wire medium ও device fixed থাকে।

Access point fixed। তাই যেখানে AdHoc Networking দরকার হয় না। তাই wireless জায়গায় adhoc wireless Network ব্যবহার করা হয়

BAM (Body Area Network): শুধু শরীরের উপর যে network. যেমন: smart watch.

Access point এবং end point এই দুইটার জন্য AdHoc use করি আমরা।

Disadvantages:-

i) power system, high powerful device use করা যায় না
→ মানে দুর্বল Algo. use করা হয় যেন charge বেশি না যায়, তাই এটার security বেশি ভালো না
যেমন: bluetooth

RFID: Example: জিনিস নিয়ে চলে যেতে থাকলে beep করে signal দিবে।

Bruteforce attack এই adhoc network break করা যায়। তাই সমস্যা সমাধান করতে করার জন্য light weight algo ব্যবহার করা হয়।
→ প্রত্যেক Algo এর হালকা version থাকে, এটা ছোট

Mobile Agent:- is a program that move one pc to another. নিজেকে produce করতে পারে। তবে এটা virus নয়, OS এর related security, বাইরে কোন intruder আছে কিনা সেটা detect করে।

Honey pot:-

08-04-2019
12th (B) day

M. J. K sir

Attacks & Threats: Slide (ch-10)

A broad category of malware:-

Ex: Fig 10.1: Example virus logic

(a) Simple virus

(b) Compression virus.

virus classification by concealment strategy:-

Encrypted virus: বাইরে থেকে বোঝা যায় না/ বোঝা যায় না।

Steal th virus: Explicitely show করবে। আসলে virus নয় তাই antivirus এরা detect করতে পারে না।

10-04-2019
12th (D) day

IK-2052 L1

S. S. S.

Security in Mobile & Wireless network:

Honeypot:

এটা একধরনের ফাঁদ। Network এর মধ্যে intruder কাজ করলে Network administrator observe করতে পারে One type of Network trap.

Page: 5 Wireless Media.

" : 6 Wireless & Mobility (Wireless communication থাকলেই যে moility থাকবে তা না, তার জন্য) Session, Mobility, Roaming → Page-06

Page: 7 Wireless Networks

Page: 11 Operation mode.

Page: 12 Infrastructure Mode.

Page: 13 ESS / BSS
- BSS → একটা service point থাকে
- ESS → একাধিক " " "

BSS এর Access point এর ~~Router~~ এর মধ্যে connection দিতে পারে।

Page 14 Operation in Infrastructure Mode.

Handover ~~आदि~~ Association ও এর

Page 15 Hand Over

Page 16 Ad Hoc mode

Page 17 IEEE 802.11 standard.

~~Page 18~~

page 19 WEP, WPA

page 20 Wi Fi

Page 21 Relationship

HiperLAN ~~কি~~ ?

Page 25 Bluetooth piconet

Page 28 conventional security Architecture.

Page 29 VPN (virtual private Network)

page 30 - - ——

page 31 Wireless user is in untrusted zone.

Page : 33 Different types of Attack.

page : 34 Attacks coithout keys.

page : 37 common attacks On WiFi LAN

5-04-2019
13th (B) day

S.S.S.

IK 2002-L2-Wifi-large(2).pdf

802.11 Basic Frame format (page 04)

Page-05, 06, 07, 08, 09, 10, 12 (WEP), 13, 14, 15, 16, 17, 18, 19, 20, 21 (পূর্বনাম), 22 (use করতে পারি), 23, 24, 25, 26, 27, 28, 29, 31, 32, 33, ~~34~~, 37.

Next class → WAPA

6-04-2019
13th (B) day

M.J.K.S.

Assignment :- → B.V. এর আগে তুমা দিতে হবে।

(i) Evasdroping
(ii) IP spoofing
(iii) Sybil Attack (Appliction এ)
(iv) Blackhole Attack (কি, example)
(v) Grayhole Attack
(vi) Password based Offline attack.
(vii) Denial of service (DOS)
(viii) Distributed DOS Attack (DDOS)
(ix) Digital Signature.

~~Code~~ Code
(a) A simple virus
(b) A compression,
Example virus Logic

Malicious soft. slide
* Including others

VIRUSES,

» structure, phase.

A compression virus.

VIRUS classification by Target.

» »

WORM (B.V.)

» phases.

» Propagation Model.

বাকি গুলান বুঝতে হবে।

PAYLOAD theft.