Authetication Application

* Kerberos protocol
Three heads
① client or principal
② Network resource
③ key distribution center

Kerberos
- trusted key server system
- centralised private-key

Firewalls vs Kerberos

Kerberos Requirements
Three approaches
① User identification
② client systems authetication themselves to serve
③ Used to prove identity for each servers.

KDS involves two servers
① Authenticate server
② Ticket Granting server

C → AS : IDC || PC || IDV
AS → C : Ticket
C → V : IDC || Ticket
Ticket = EKV ||IDC || ADC ||

IMP ① Once per user logon session:

① C → AS : IDc || IDtgs
② AS → C EKC [Tickit tgs]

Scheme
- Avoid plain text passwords
- Intro TGS.

② Once per type of service

③ C → TGS : IDc || IDv || Ticket-tgs
④ TGS → C : Ticket v

③ Once per service session:

⑤ C → V : IDc || Ticket-v

Ticket tgs = EKtgs [IDc || ADc || IDtgs || TS1 || Lifetim
Ticket v = EKv [IDv || ADv || IDv || TS2 || lifetime 2

* Kerberos Realms

① C → AS ① Request tickit for local T
② AS → C
③ C → TGS
④ TGS → C
⑤ C → TGSrem
⑥ TGSrem → C
⑦ C → Vrem

Kerberos version 5
Due to environments shortcomes.

1)
2)
3)
4) Tickit lifetime
5) Autheticate lifetime
6) Interrealm autheticatio

Due to technical diffciencies
① Double encryption ② PCBC encryption
③ Session keys ④ Password attacks

* weakness and solutions

20/09/24

* kerberos brute force

* ASREPRoast

	SSL	kerberos
①	Public	Private
②	certificate based Asychronous	trusted third party Synchronous
③	Ideal for WWW	neworked environment
④	Key revocation requires revocation server to keep track of bad certificates	④

* ~~Xeo~~ X.509 Authetication service
- Internationally accepted
- how to construck public key certificate

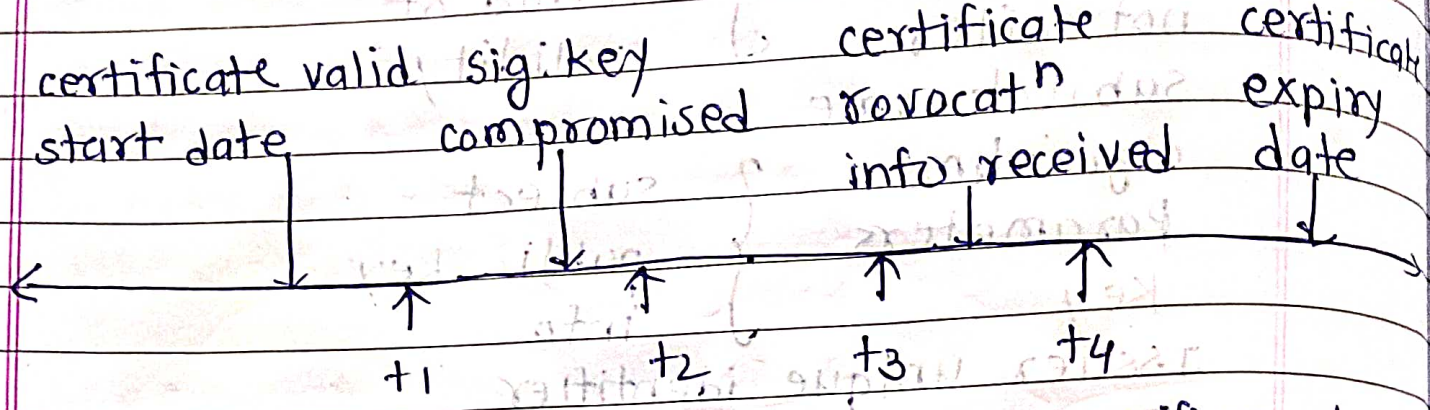
* Fields in certificate

* ~~X.5~~ X.509 certificates
Version
certification serial number
algorithm

Date.

Parameters
Issuer name
not before } Period of
not after } validity
subject name
algorithms } subject
Parameters } public key
Key } info
Issuer unique identifier.
~~Extension~~
subject unique identifier
Extensions
algorithms } signature
parameters }
encrypted

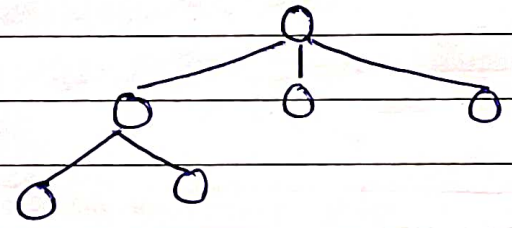
Certification Revocation vs signature Acceptance Log time



Case	sig. gen^n time	sig. verif^n time	Does verifier accept sig?	should verifier accept
1	t1	t3	Y	Y
2	t1	t4	N	Y
3	~~t3~~ t2	t3	Y	N
4	~~t4~~ t2	t4	N	N

Obtaining certificate

Internet certificate Hierarchy



X509 PKI - Technical view

Basic components

CA

RA

certificate distribution system }

Date.

PKI Infrastructure - Issuance
PKI - Usage

Types of certificates:
① Organizational certificates
② Residential certificates
③ Personal certificates

signature) Principal need not

Authetication procedure
① One way
② Two way
③ Three way

Certificate extensions
key & policy info

* Identity based encryption (IBE)
* PKI Architures
① - central trust relation - ① Architeures
- realiability

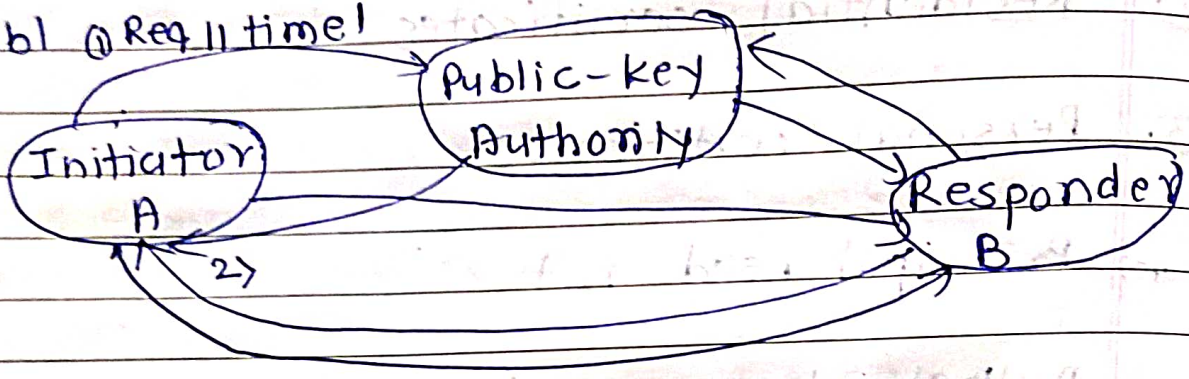
② - Limited no. of user. - ② Architectures

③ - Dense web of trust - ③ Mesh-based PKI

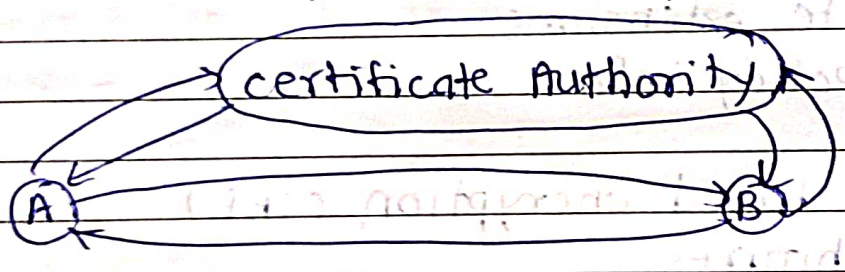
④ Bridge-based PKI

* Key management in cryptosystems

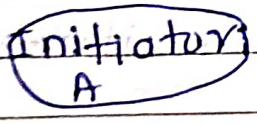
Public Announcement
Public available directory
IMP Public key Authority with dig.
- does not req. real time access
Publ @ Req'd time!



Public key certificates
- without real-time access to public-key authori
(key exchange
- binds identity to public key



* Public key distribution of secret keys
* Simple secret key distribution



* Hybrid scheme
- IBM Mainframes
  3 level encryption
  ① Keys^1, ②user^2 and ③keys^3

- Performance, Backward compatibility

* Diffie-Hellman key exchange
- It is not used for secure communication
- It is used for secure communication of keys only
- Used in no. of commercial products.

Primitive roots
- Euler theorem: $a^{\phi(n)} \bmod n = 1$
- $a^m = 1 \pmod n$, $\gcd(a, n) = 1$
  - must exis for $m = \phi(n)$, but may be smaller.
  - once power reach m, cycle will repeat
- if smallest is $m = \phi(n)$ then a is called primitiv root
- If P is prime, the successive power of a generate the group mod p.

- These are useful but relatively hard to find.

Table - Powers mod 19

* Discrete logarithms
  Diffie - Hellman setup

show that 2 is primitive root of 11.

$p = 11, \quad a = 2$

$2^1 \bmod 11 = 2$

$2^2 \bmod 11 = 4$

$2^3 \bmod 11 = 8$

$\vdots$

$2^{10} \bmod 11 = 1$

$b \equiv a^i \bmod p \quad$ where $0 \le i \le (p-1)$

The exponent i is referred to as discrete logarithm or index of b for base $a \bmod p$.

- each user (eg. A) generates their key
  - choose a secret key (no) $X_A < q$
  - compute their public key: $Y_A = a^{X_A} \bmod q$
- each user make public that key Y_A.

* Diffie-hellman key exchange

$K_{AB} = a^{X_A \times X_B} \bmod q$

$= Y_A^{X_B} \bmod q$ (which B can compute)

$= Y_B^{X_A} \bmod q$ (which A can compute)

Alice & Bob wants who wish to swap keys: agree on prime $q = 353$ and $a = 3$

select random secret keys:

- A choose A $X_A = 97$, B chooses $X_B = 233$

compute public keys:

$Y_A = 3^{97} \bmod 353 = 40$ (Alice)

$Y_B = 3^{333} \bmod 353 = 248$ (Bob)

- Compute shared session keys as:

$K_{AB} = Y_B^{X_A} \bmod 353 = 248^{97} \bmod 353 = 160$

$K_{AB} = Y_A^{X_B} \bmod 353 = 40^{233} \bmod 353 = 160$

Q.1 A & B users use D-H key exchange technique with a common prime $q = 71$ and primitive root $a = 7$

A) If user A has private key $X_A = 5$, what is A's public key Y_A?

B) If user B has private key $X_B = 12$, what is B's public key Y_B?

c) what is shared secret key?

$q = 71$, $a = 7$

Q. 2 Consider a D-H scheme with a common prime $q = 11$ and primitive root $a = 2$

a) If user A has public key $Y_A = 9$, what is the A's private key $X_A = 6$

b) If user B has public key $Y_B = 3$, what is shared secret key $K_B = ?$

* Message Authentication and Hash functions.

Message Authetication func
- Message encryption
- Message authetication code

MAC ≈ cryptographic checksum
For n bit Mac: 2^n possible Mac's
For k bit key: 2^k possible keys.

eg. 100-bit message & 10 bit MAC
2^{100} diff message, but 2^{10} diff mac.

on avg, each mac value is generated by total of $2^{100}/2^{10} = 2^{90}$ diff messages.

For 5-bit key, $2^5 = 32$ diff mapping from set (msg) to set (MAC values)

Internal and external error control
~~In both~~
In internal it takes the encryption but external no encryption is their.

IMP as short note Application MAC

on avg rounds $K = R \times n$

80 bit key & 32 bit MAC

Round 1:

$2^{80-32} = 2^{48}$ possible keys

Round 2:

$2^{80-2\times32} = 2^{16}$ possible keys

Round 3:

$2^{80-3\times32} = 2^{80-96} =$

should produce only a single key which must

Using symmetric ciphers for MACs.

* Hash functions

short note for ese

* Requirments of hash functions

Birthday problem

what the chances that two people in a class of 43 students have same birthday?

Approximation solution:

$p = 1 - e^{-\frac{k^2}{2N}} = 1 - e^{-\frac{43^2}{2\times}}$

In a room of k people

$$q = \frac{366}{365} \times \frac{364}{365} \times \cdots \frac{365-(k-1)}{365}$$

$$q = \frac{365!}{(365-k)!}$$

If the no of m birthday, the coordinating n of hash function is

hash

$$n = 2^m$$

$$k \approx \sqrt{n} = 2^{m/2}$$

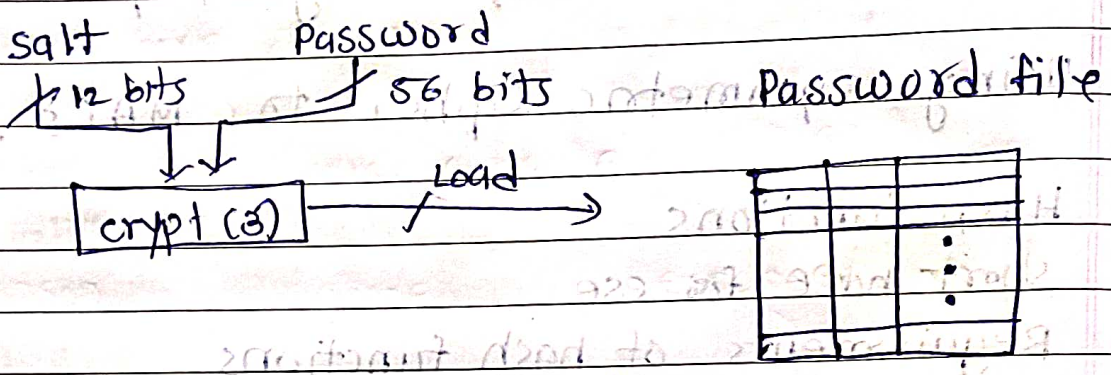
Page No.
Date.

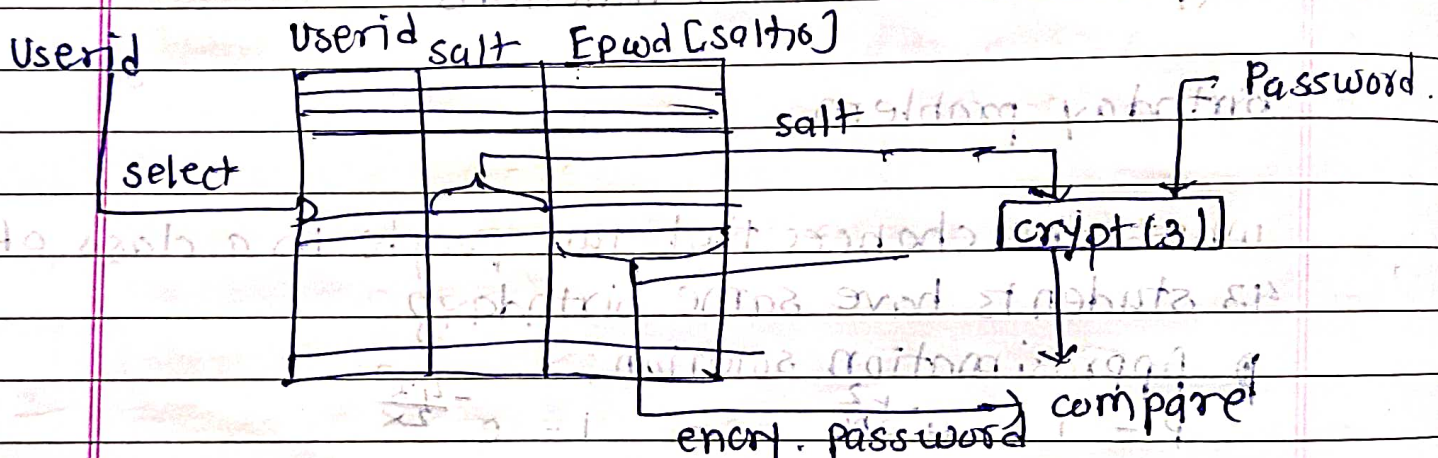
Password protection

Keys vs passwords

Markov model

Unix Password Scheme





Before this lec ppt uploaded (absent for Tes NCET)

Page No.
Date. 04 10 24

* Intruders

Black hat — ④ Analyzing
white hat — ① Remembering
Blue hat — ⑤ Evaluating
Greeen hat — ⑥ Creating
Red hat — ② Understanding
Yellow hat — ③ Applying

Types of Hackers
* Professional hackers
- Black hats
- White hats

* script kiddies
- Mostly kids/students

* Underemployed
* Corporate hackers

* Criminal Hackers
* Disgruntled employees

Three classes of intruders
① Masquerader
② Misfeasor
③ clandestine user

Events of interest to an IDS

variable monitored	Event of interest	Possible Attack

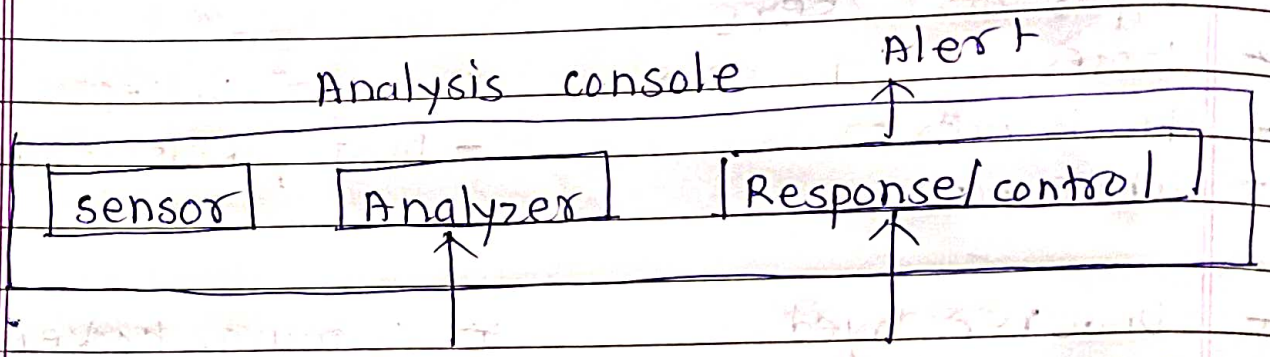
CASE
entropy - Amount of info
entropy of plaintext + entropy of crypt key
= entropy of ciphertext (eq-1)

Date.

case ①: LHS < RHS.
- derives only one plaintext.

case ② RHS < LHS
- can go for multiple plaintext and all are valid one.

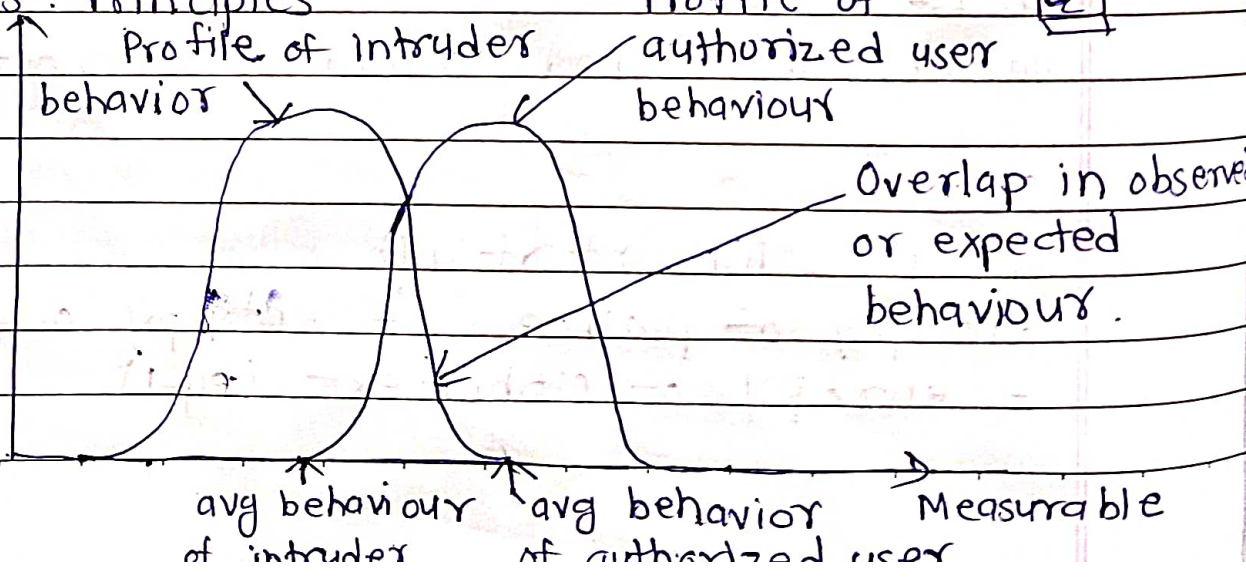
* Intrusion Detection.
Architecture of IDS



~~Intrusion detection system~~
(in explain. dig).

* Intrusion detection system
Dig

* IDS: Principles



tool
pasive working
active

Page No.
Date.

Mathematical description of IDS.

* IMP Approaches to intrusion detection
what are
statistical anomaly detection
attempts to define normal/expected behavior
① Threshold - use for freq of occurances for various events
② Profile based

Rule based detection
① Anomaly
② Penetration detection

* Base - rate fallacy
* IDS & IPS placement

* Honeypot (short note)
Honeypot Advantages

Honeypot Types
Low Interaction } diff
High Interaction }

07/10/24

* Web traffic security approaches
SSL architecture
(Parameter not imp)

SSL Record Protocol steps (r

Handshake protocol
(Phase 1: Establish security capabilities
(x not expected in exam)

Page No.
Date.

IMP PYQ. (IMP) on this topics

- SET components (bank, account)
- Dual signature related to SET

- SET environment
  customer } fig imp
  Merchent }

SSL	TLS
secure socket layer	Transport leyer security
supports Fortezza algorithm (encry, hashing, DSA)	Does not support Fortezza
common in the 3.0 version	1.0 version

Message digest is used to create secret

* L = specific to the os and communication link
  L = comm b/w of victim link (bits/sec)
  B = max. no. of buffers reserved for TCP connection
  T = max amount of time (sec) that buffer can be reserved for half open TCP connection

~~To charact~~

$R \times P >= L$

$R \times T >= B$

Assume that size of SYN packet including MAC header is 84 bytes

Let victim's inbound link capacity is 100 Mbps

$P = 84B = 84 \times 8 = 672$ bits, $L = 100$ Mbps $= 100 \times 10^6$ bits

Q1 To saturate the link what should be R?

$\Rightarrow R \times P >= L \quad R >= \frac{L}{P} = \frac{100 * 10^6}{672} = 148809.5$

$R = 150{,}000$ packet/s

Q.2 If total 8000 buffers are working for 9 sec what R is preferred?

$B = 8000$

$T = 9$

$R \times T >= B$

$R >= \frac{B}{T}$

$R >= \frac{8000}{9}$

$R >= 888.889$

$R = 900$ packets/sec.

Q3 For each connection TCP reserves 300 bytes of buffer space, what should be typical value of R?

~~$P B = 300 \times 8 = 2400$ bits~~

$P = 84B = 84 \times 8$

Buffer size $= B \times 300$ bytes $= 800 \times 300 \times 8$ bits

$R >= \frac{(8000 \times 300 \times 8)}{84 \times 8}$

$R = 29000$ packet/sec.

What is firewall

Firewalls - Packet filters

Packet filtering routes are:
① simple
② Transparent to use
③ very fast

Dynamic / statful packet filters

Firewalls- Application level Gateway (or Proxy)
Application level

Adv, Dis, Apph

Bastion point
Bastion Host- characteristics.
- Highely secure for apph-level or circuit-level gateway.
- operating system, making trusted systems.
- Additional authentication
- Audit information

Network Address Translation.
Firewall configuration
(single-home bastion system)

Firewalls 2 systems
①
②

2) Dual home bastion system
3) screened - subnet firewall system

Trusted systems
Bell LaPadula (BLP) model)
case: trojen

firewalls
type of firwalls
configurations
access control
rusted systems

Date: 11/10/24
Day: Friday

Passwords security levels

Passwords Brute force Attacks.
Who are cyber - criminals?
Type I: Cybercriminals - hungry for recognition
Type II: Cybercriminals - not intrested in recognition.
Type III: Cybercriminals - the Insiders.

Cyber Breach types
Cyberstalking - chatting.
Cyberterrorism -
Cyberporn -
Cybertheft -
Cyberlandering -
Cybervandalism -
Cyberlaundering -
Cyberfraud -
Cybertresspassing -

How Computers are involved in Attacks?

	Narrow sense	Broad sense	
Role of computer	computer as object	computer as a tool	computer as an ~~text~~ context or environment

examples

Power analysis attack
Power traces of DES
DPA result example
Memory attacks
side channel attacks
Prime factorization
$n = a \times b \times c$
prime factorization
$300 = 2^2 \times 3^1 \times 5^2$ $18 = 2^1 \times 3^2$ hence
GCD $(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$
Determine the GCD by comparing the prime factorization of

Fermat's theorem
$a^{p-1} \equiv 1 \pmod p$
where p is prime and gcd $(a, p) = 1$
$a = 7$, $p = 19$
$7^2 = 49 \equiv 11 \mod 19$
$7^4 = 121 \equiv 7 \mod 19$
$7^8 = 49 \equiv 11 \mod 19$
$7^{16} = 121 \equiv 7 \mod 19$

$a^{p-1} = 7^{18} = 7^{16} \times 7^2 = 7 \times 11 = 1 \mod 19$

Euler Totient function $\phi(n)$

complete the table

$\phi(p,q) = \phi(p) \times \phi(q)$ if $p \neq q$

$= p \times \phi(q)$ if $p = q$

N	$\phi(N)$
1	1
2	1
3	2
$4 = 2 \times 2$	2
5	4
⋮	
25	20

How to do question

N	$\phi(N)$	N	$\phi(N)$
1	1	$16 = 4 \times 4$	8
2	1	17	16
3	2	$18 = 3 \times 3 \times 2$	
$4 = 2 \times 2$	$2 = 2 \times 1$		
5	4		
6	2		
7	6		
$8 = 4 \times 2$	$4 = 2 \times 2$		
$9 = 3 \times 3$	$6 = 3 \times 2$		
10	4		
11	10		
$12 = 4 \times 3$	$4 = 2 \times 2$		
13	12		
14	6		
15	8		

short note

Elliptic curve Cryptography

Public key

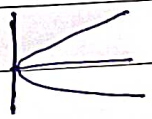
Why ECC?

- shorter key length
- lesser computational
- low power requirement
- secure

General form of EC

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

$y^2 = x^3 - 1$



Ref: DSA Signature signing & verification

sig never is 2 parameter, never be 1 parameter

Signing

Verification

Security of ECC

To ~~pro~~

William Stallings PPT

Advantages and limitations of ECB

- chance of error becomes less

* Cipher Block Chaining

dig $C_i = DES_{K_1}(P_i \text{ XOR } C_{i-1})$

$C_{-1} = IV$

user: bulk data encryption, authetication

Message padding

Advantages and limitations of CBC

* Cipher Feedback

stream mode (of bits)

E-E EE Ladder

* Advantages and limitations of CFB

* output Feedback (OFB)

* Counter (CTR)

* ECB

* CBC

* CFB

* OFB

* CTR

Advantages of CTR mode

H/W efficiency

S/W efficiency

Preprocessing

Limitations of CTR.
confidentiality

which

c) ii) &

Application: PCBC mode
kerberos v4

Tutorial solved

complete the table -- comment on CIA priorities.

Why CBC decryption can be parallel?
A major advantage of CBC mode is that while encryption must be performed sequentially

An is Public key cryptography and RSA
Private key cryptography

* source A source B
Dig
Public key cryptosystem

$Z = E_{KUb}[E_{KRa}(X)]$
$X = D_{KUa}[D_{KRB}(Z)]$

* Public-key Applications
* Trap door function.

Page No.
Date.

* RSA Algorithm
RSA Key ~~step~~ Setup

- selecting 2 large prime no. P & q
  N = P.q.
  -note $\phi(N) = (P-1)(q-1)$
- selection at random the encryption key e
  - where $1 < e < \phi(N)$, $\gcd(e, \phi(N)) = 1$

$5^7 \bmod n$
$= [(5^2 \bmod n) \times (5^2 \bmod n) \times (5^2 \bmod n) \times (5^1 \bmod n)] \bmod n$

Q.1 Perform encryption and decryption using RSA algorithm for following

① P=3, q=11, e=7, M=5
N = 3×11 = 33
$\phi(N) = 2 \times 10 = 20$

$d = e^{-1} \bmod (P-1)(q-1)$
$= 7^{-6} \times \bmod (20)$
$= 1$

② P=5, q=11, e=3, M=9
N = 5×11 = 55
$\phi(N) = 4 \times 10 = 40$
d =

P=7, q=11, e=17, M=8

P=11, q=13, e=11, M=7

P=17, q=31, e=7, M=2