(5) eg digital documents

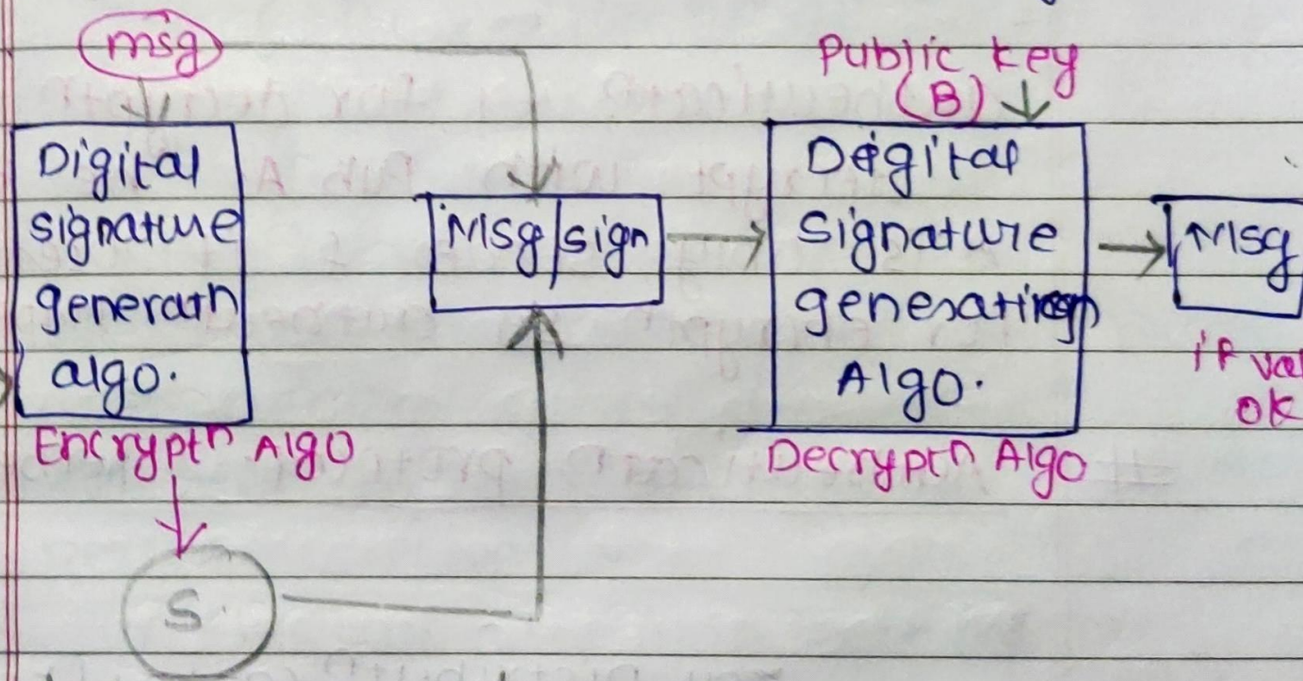
Chapter- 4.

Date
Page

(1) type of electronic sig (2) It's mathematical algo used to validate the authenti

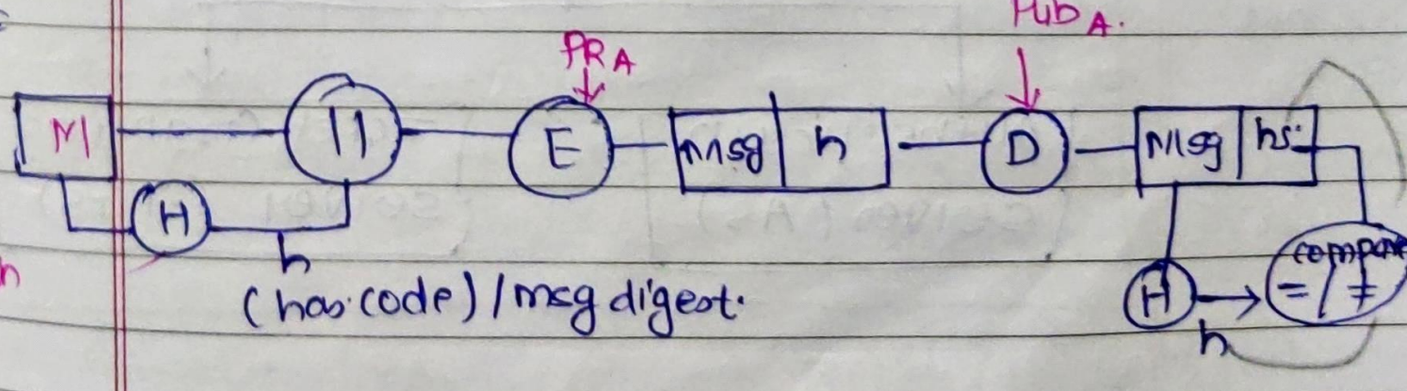
Digital signature: 4 S of msg.

(1) impt Role in e-comme, Online tracth
(2) based on assymetric key
Encryptn - private key
decryption - public key.
(3) used for msg (authenticatn) & non repudiation & msg integrity. (correct person) (cannot deny)
(4) Not used for confidentiality.



digi. sign generated

OR



(b) Also provide msg integrity.
If 3rd party attack & msg change than at receiver end we will not get exact msg ⇒ TO avoid this happen.

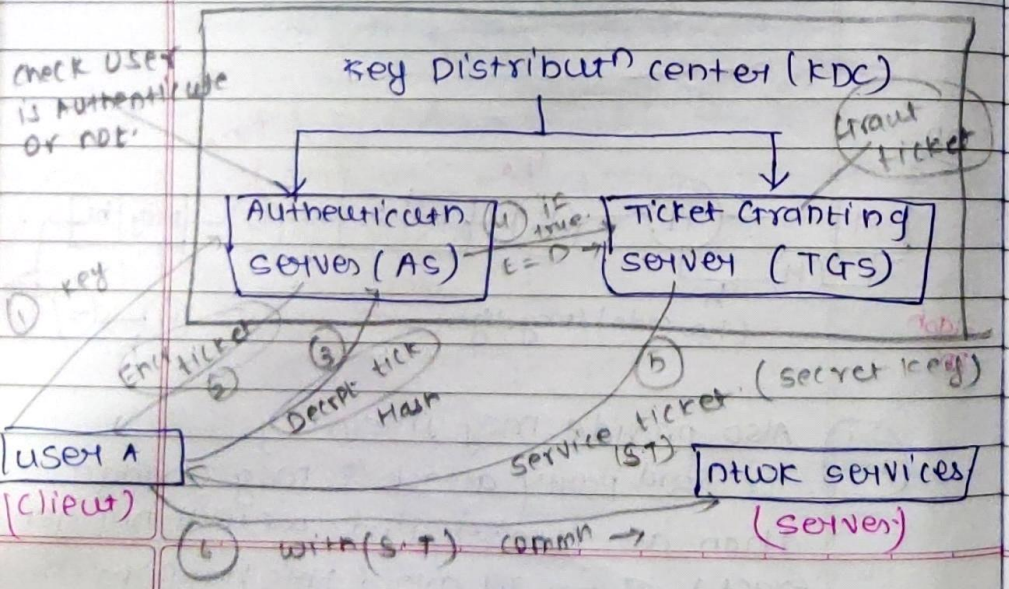
D·sig·→ it provide msg integerit ⟹ acheived using Hashing conlept using msg digest / hash value.

when we sign a document digitally, we send signature as seperate document. & snder send 2 doc → msg & sign.

Step { ① Key generatn Algo → To generate- Pvt key ② signing algo → i/p → msg / Pvt key, o/p → Digital sig ③ verifying algo → using Pub key & sign.

authenticatn → for decryptn B (Receiv) decrypt with Pub A· he know A is only sender & it uses Pvt A· for encryptn so authentn happened.

Authenticatn protocol· (kerberos protocol)



① A·prot· → If you want to use any services of a perticular network. so that ntwk provide services only if you are our trusted user

A·P· check whter user is Authented or n if ✓ then ntwk provide services viewe

② follow client server Archit·

③ symutric key·

④ Requires a third party for key (KDC) → dB of all secret key.

Working:

① In KDC center 2 servers → AS & TGS

② Now, user want to Access the services of netwk·

③ For Accessing ntwk user has to be author person· (In KDC)

④ For checking user A is auth· or not·

⑤ Now, user A send msg that I want key to Access the services of ntwk·

⑥ Now KDC transfer to AS to check Authiti

⑦ AS send ticket to (A) which is Encrypte

⑧ user will Decrypt the ticket· & get hash code

⑨ Now again Decrpted ticket (Hcode) send back to AS· AS will check authencity

⑩ If user Decrypted correctly that means it's certified user / or Authenticate user.

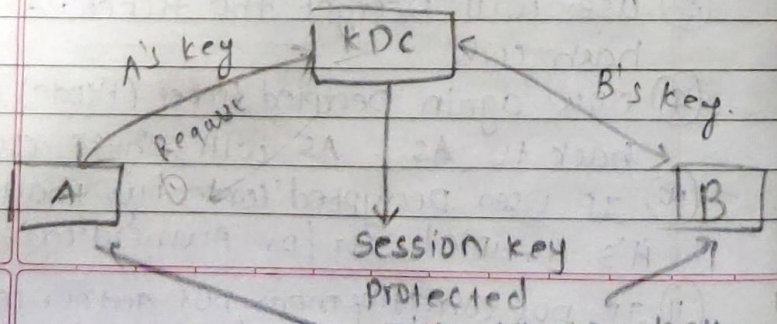
⑪ If not correctly means not authorised & not send any anything to user A·

(ST)

(12) Now AS having services ticket which is send to TGS for Granting.
(13) TGS send ST which is secret key to user A.
(14) Now user A can Access the services of perticular ntwk with scret key.

Needham Scheroeder protocol (NCP)

(1) It's symmetric key protocol
(2) uses sym. algo. for encryptn.
(3) It provide confidentiality for commncatn with KDC
  (I) Each group in ntwk share secret key known as Master key with KDC → (center authority)
  (II) KDC generate limited time keys for connectn betn 2 grp known as session key. → (scrt key with time limit)
  (III) session key are protected by master key during distribution.



Working.

(1) user A want to commn to user B.
(2) It send a Request msg to KDC
KDC is db of all user secret key. it store all secret key.
(3) A → KDC : $ID_A \| ID_B \| N_1$
A send KDC with
ID_A = user A identificatn, ID_B = for B
N = Nounce ⇒ some simple msg.
K_s = session key,
K_A ⇒ Master key of A, $K_B = M(k)$ for B
(secret key)

(2) $KDC \rightarrow A : E(K_a, [K_s \| ID_B \| N_1 \| E(K_b, [K_s \| ID_A])$

Now KDC send Reply user A with Session key i.e Master key of A & B i.e k_a & k_B which is in encrypted

Decrypt
user A ~~Encrypt~~ the msg with Master key & get session key (K_S), ID_B & N_1

Blw part

But it can't decrpt the 2nd part ( )
Becoz it's encrypted with Master key of B. & user don't have Master key (sect k.g.B)

(3) $A \rightarrow B : E(K_b, [K_s \| ID_A])$

Now user A send Encrpid part of B to B.
B will decrpt with Master key and get Session key & identificatn of A.

(4) $B \rightarrow A : E(K_S, N_2)$

Now Authecatn acheived, so B send to A encrypted session key & Nouch B nount B => ⊛ which is created by User B.

(5) $A \rightarrow B : E(K_S, F(N_2))$

Now User A Reply the Nource using the session key (secret key) in Encrypted formate.
& User B get decrpt that Replay of Nonce (N_2).

Still it's valunerable ⇒ of replay Attack

How it's valn⇒

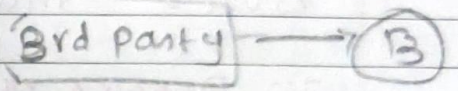
(1) when user A commn to B, in (3) step msg captured by any 3rd party & can take the 3rd step and replay the 3rd step to user B.

(2) After geting 3rd step User B decrpt the msg & get sess k (K_S) & ID_A: bt it and send back to user A.
bt actually it's not sending to A.
it's sending it 3rd party.
and user B which is unware about this tings.

This is called Replay attack, start here.

(3) when in stp 4 B send the session key & Nonce N_2 to A.
so same time 3rd party can get N_2 also. & it get full idea of working A.

User B A comn with 3rd party instead of B. & User B getting msg from 3rd ~~inst~~ part instead of A.



Denning proposes overcome this's weakness by Applying time stamp in step (2) & (3)

soln by Denn⇒

(1) $A \rightarrow KDC : ID_A \| ID_B$.

(2) $KDC \rightarrow A : E(K_a, [K_S \| ID_B \| T \| E(K_b, [K_S \| ID_A \| T])])$

(3) KDC Reply to User A with session msg of Both A & B with Master key in Encrypted form.
User A will ~~Enter~~ Decrypt the Msg with Master key & get K_S (session k) & IDB.
& one timestamp 2nd part not decrpt by user A.

(3) $A \rightarrow B : E(K_b [K_S \| ID_A \| T])$
A send to B & B decrpt msg with Master key & get ID_A & Timestamp

(4) B → A : E (Ks, N1)
A → B : E (Ks, F(N1))

Timestamp follow & Check

| clock - T | < Δt1 + Δt2

T = sending time

Δt1 = estimated time from (KDC) — local time (A or B)

Δt1 = KDC — local time (A & B)

Δt2 = N/w delay time.

In Denning Method 1 error occur. that no one have the exact time

e.g. User A T.stam = 12.30 pm

e.g if ~~User A send~~ B = 12.29 pm.

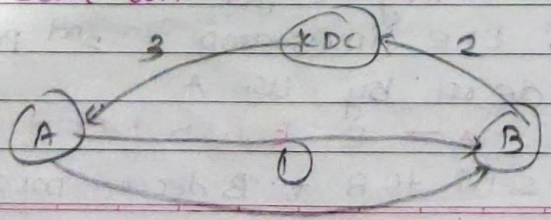
It occurs non accuracy of sending the date in same timestamp.

or If KDC = 12 pm

but A = 12.02 | B = 12.3

Gong = refer to synchronyse the time stamp.

i.e synchronize ~~KD~~ user timest. to KDC T.S everytime. so result will be accurate.



4. One-way A. is more suitable in ~~this~~ NCP

(1) A → B : IDA || Na

(2) B → KDC : IDB || Nb || E(Kb, [IDA || Na || Tb])

In 2nd stp B → KDC with IDB, Nb with Master key of B [IDA, Na, TB] in encrypted formated.

KDC decrpt with Master key of B.

(3) KDC → A : E(Ka, [IDB || Na || Ks || Tb] || E(Kb, [IDA || Ks || Tb]) Nb

(4) A → B : E(Kb, [IDA || Ks || Tb]) || E(Ks, Nb)

(5) Now user B decrpt both part & get IDA, Ks, Tb, with Master key Kb & also get Ks (session key & nonce

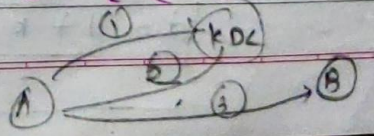
This is the more sequne way to comm with both A & B with KDC.

4. One way authentication. It's not having 4th & 5th step

(1) A → KDC : IDA || IDB || N1

(2) KDC → A : E (Ka, [Ks || IDB || N1 || E (Kb, [Ks || IDA])])

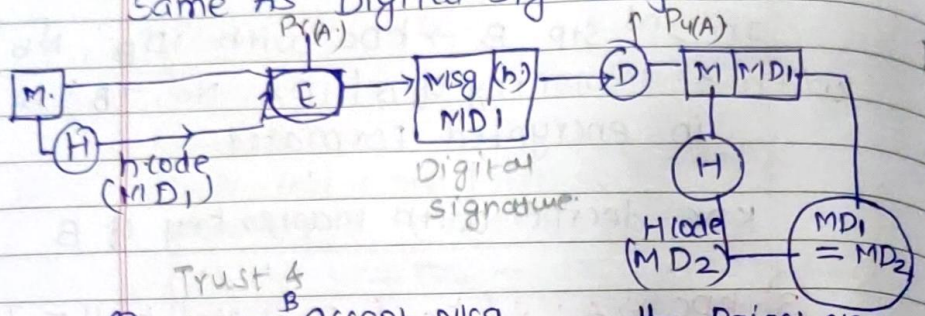
(3) A → B : E (Kb, [Ks || IDA]) || E(Ks, M)



publicity - Poster/writer - Blog (Manoj)
Register link - (Web)

Digital Signature ⟹ RSA

Same As Digital sig. diagram.



Trust & $=^B$ accept Msg, # Reject Msg. original Msg

(I) RSA sig. is used for signing & verify a Msg called RSA d.sig.

(II) only sender's private and public key used for encrptn & decreptn

(III) Sender user own pvt key to sign doc. Rec. uses sender pub key to verify doc.

(IV) For siging & verify same ~~para~~ Functn but diff. parameter.

Algo: (1) p, q, 1
(2) $n = pq$, (3) $\phi(n) = (p-1)(q-1)$
(4) $1 < e < \phi(n)$ $\gcd(\phi n, e) = 1$
find e.
(5) Find d, $ed \bmod \phi(n) = 1$

$$d = \frac{1 + k(\phi n)}{e}$$

If sig. & verify same than ~~use~~ its ~~to~~ right msg.

Signer

(6) For signing. (n, d) = RSA pvt key.
(n, e) = signer pub key

$$S = m^d \bmod n$$

(7) For verifying

$$m = s^e \bmod n$$

(n, e) signer Public key.

m = Verifying msg.

Plaintax $X = 22$.

ex. (1) $p = 3$, $q = 17$. e = public key
(2) $n = pq = 3 \times 17 = 51$ d = private key
(3) $\phi(n) = (3-1)(17-1)$
$= 2 \times 16 = 32$
(4) choose e,
$\because \gcd(e, \phi(n)) = 1$

Choose e, such that co factor of $\phi(n)$
co-prime = should not ~~equal~~ multiply by factor $\phi(n)$ & not divide by $\phi(n)$

$\phi(n) = 32 = 2 \times 2 \times 2 \times 2 \times 2$

so e not multiply by 2 & not divide by 32

prime no, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21 ... 31
we choose, 3 as e.

$e = 3$

$9 = 1 \times 3$ 1 common
$32 = 1 \times 2 \cdots$ gcd = 1

(5) Find d. $ed = \mod(\phi n)$

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

$d = \frac{1 + k(\phi n)}{e}$

OR

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

IF k=2 $d = \frac{1 + 2(32)}{3} = \frac{65}{3} = 21.\cdots$

k = 5 $\frac{160+1}{3} = \frac{161}{3} = 53\cdots$

k = 9 $\frac{288+1}{3} = \frac{289}{3} = 76.\cdots$

k = 11

$3 \times d \bmod (\phi n) = 1$

$3 \times d \bmod (32)$

$3 \times 11 \bmod 32 = 1$

$d = 11$

$3 \times 3 \bmod 32 = 9$

$15 \bmod 32 = 15$

$3 \bmod 32 = 3$

$6 \bmod 32 = 6$

$9 \bmod 32 = 9$

public key $(n, e) = (51, 3)$

private key $(n, d) = (51, 11)$

(II) Sign = $S = M^d \bmod n$

$= (22)^{11} \bmod (51) = 8$

(III) Verifn = $m = S^e \bmod n$

$= (8)^3 \bmod (51)$ $\neq 8$

(6) El-Gamal. ⇒ Same as Diffie-H.

(1) Select prime no. q

(2) Select primitive root α

(3) Generate Random integer X_A. $1 < X_A < q-1$

(4) Find $Y_A = \alpha^{X_A} \bmod q$.

(5) Find key for user A.

prvt key = X_A. ⇒ Decryptn

Public key = $\{q, \alpha, Y_A\}$. ⇒ Encryptn

(6) Find Hash code (m/h) for plaintext (M)

$h = H(M)$ $0 \le m \le q-1$

(7) Find Random integer k

$1 \le k \le q-1$ and $\gcd(k, q-1) = 1$

(8) Find S_1 & S_2,

$S_1 = \alpha^k \bmod q$.

$S_2 = k^{-1}(h - X_A \cdot S_1) \bmod n$

(9) We got signature pair (S_1, S_2)

(10) From User B side. Find V_1 & V_2

$V_1 = \alpha^h \bmod q$

$V_2 = (Y_A)^{S_1} \cdot (S_1)^{S_2} \bmod q$.

if $V_1 = V_2$ ⇒ signature is valid

$V_1 \neq V_2$ = not valid.

① e.g. Let $q = 19$.

② (primitive root) $\alpha = 10$

③ $X_A \ldots (1 < X_A < q-1)$ $(1 < X_A < 18)$

Let $\boxed{X_A = 16}$

④ $y_A = \alpha^{X_A} \bmod q = (10)^{16} \bmod (19)$

$\boxed{y_A = 4}$

⑤ FOR A:

Pvt key $= X_A = 16$

pub key $= (q, \alpha, y_A) = (19, 10, 4)$

⑥ Hash code (h) for plaintext (M)

$h = H(M) : 0 \le h \le q-1$

$= 0 \le h \le 18$

let. $\boxed{h = 14}$ $0 \le 14 \le 18$

⑦ Find Integer k

$\gcd(k, q-1) = 1$, $\gcd(k, 18) = 1$

$18 = 2 \times 3 \times 3$

k should not factor of 18 & not divide to 18

so prime no. of $\boxed{k = 5}$

⑧ Find S_1, S_2 $\quad S_1 = \alpha^k \bmod q$

$= 10^5 \bmod 19 = 3$ //

$S_2 = k^{-1}(h - X_A \cdot S_1) \bmod q-1$

$= k^{-1}(14 - 16 \times 3) \bmod 18$

$= 5^{-1}$ (

$\frac{5 \times i}{12} = 1$ (Remainder)

$k^{-1} = k^{-1} \bmod q-1$

$= 5 \times ? = 1 \bmod (18)$

$k^{-1} = \frac{5 \times ? = 1}{18}$ | or $k \times i \bmod 18 = 1$

Reminder 1

$= \frac{5 \times 11}{18} = 1$

$\boxed{k^{-1} = 11}$

$S_2 = 11\,(14 - 16 \times 3) \bmod 18$

$\boxed{S_2 = 4}$

For B's end

$v_1 = \alpha^h \bmod q$

$= [10]^{14} \bmod 19 = 16$

$\boxed{v_1 = 16}$

$v_2 = (y_A)^{S_1} \cdot (S_1)^{S_2} \bmod q$.

$= 4^3 \times 3^4 \bmod 19$

$= 5184 \bmod 19$

$\boxed{v_2 = 16}$

$\therefore \quad v_1 = v_2$

Signature is valid.

$t = 1$ to 18. $\quad t = 13$, $\alpha = 2$

Pvt key $X_A = 3$ //

msg (PT) $= 11$

$k = 2$

* IA.

Q. (1) $q = 13$ — given

(2) ~~$h = 11$~~ $\alpha = 2$ — given

(3) x_A — $(1 < x_A < q-1)$ $(1 < 3 < 12)$

$\boxed{x_A = 3}$

(4) $y_A = \alpha^{x_A} \bmod q = (2)^3 \bmod (13)$

$= 8 \bmod 13 = 8$ //

(5) For A. Pvt key $x_A = 3$

Pub key $(q, \alpha, y_A) = (13, 2, 8)$

(6) Hash code (h) For Msg (plain text)

$h = H(M) = 0 \leq h \leq q-1$

$0 < h \leq 12$

(given) $h = 11$ (try to take always prime no.

(7) Find k, gcd (k, q-1), gcd (k, 12)

2 | 12
2 | 6
3 | 3
1

Factor 12 = 2 x 2 x 3 always

so $\boxed{k = 5}$ — Prime factor

k It not factor from 12 & not divide to 12

(8) Find s_1, s_2

$s_1 = \alpha^k \bmod q = 2^5 \bmod (13)$

$= 32 \bmod (13) = 6$ //

$s_2 = k^{-1} (h - x_A \cdot s_1) \bmod (q-1)$

$k^{-1} = k^{-} \bmod (q-1)$ o, $k^{-1} x ? = \bmod (12)$

$k^{-1} = \frac{5 \times ?}{12} = 1$

Or $\boxed{5 \times i \bmod 12 = 1}$

$k = \frac{5 \times 5}{12} = 1$, $\frac{25}{12} = 1$

$\boxed{k = 5}$

$s_2 = 5 (h - x_A \cdot s_1) \bmod (q-1)$

$= 5 (11 - 3 \times 6) \bmod 12$

$= -35 \bmod 12$

$\boxed{s_2 = 1}$

For B's end.

$v_1 = \alpha^h \bmod q.$

$= (2)^{11} \bmod (13)$

$= 7.$

$v_2 = (y_A)^{s_1} \cdot (s_1)^{s_2} \bmod q$

$= (8)^6 \cdot (6)^1 \bmod 13$

$= 262144 \times 6 \bmod (13)$

$= 7.$

$v_1 = v_2$

Hence. signature is valid //

Schnorr Digital Sig.

6 time faster than Elgamal algo.

(1) It's faster than Elgamal Alg. becoz it minimize the msg size and generate sig.

(2) It doesnot depend upon. Msg.

$p = 2^{1024}$ ⇒ 1024 bits no.

$q = 2^{160}$ ⇒ 160 bits numbers.

i.e length of SHA-1

Schnorr Digital sig.

Ref. Diag from notes.

① Parameters , p, q, a, s, v, r, x, y.

Choose ① p = prime no.

② q = prime factor of p-1

choose q value such that it's divide by p-1

Choose ③ a = , → $a^q = 1 \bmod p$

global public key ⇒ {p, q, a}

④ choose s .... $0 < s < q$

private key = {s}

⑤ user public key (v) = $a^{-s} \bmod p$.

For signature create. ① choose, r ... $0 < r < q$

find $x = a^r \bmod p$

② concatenate ⇒ $e = H(M \| x)$

③ compute $y = (r + s \cdot e) \bmod q$

So signature consist of pair (e, y)

Verification

① find $x' = a^y v^e \bmod p$.

② verify $e = H(M \| x')$

$x' = a^y v^e = a^y a^{-se} = a^{y-se} = a^r = x \bmod p$

Hence, $H(M \| x') = H(M \| x)$.

DSS – Digital signature Standard