



Subject Incharge: Prof. Sarala Mary Page No. 1

# A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering Data Science



Department of CSE-Data Science | APSIT

Semester: VI Subject: CSS Academic Year: 2028- 2029
ELGAMAL DIGITAL DIGITAL DIGITAL
* The Higamal digital signature scheme sums from the
ElGamal cyptosystem based upon the security
I I V V D ALL AN AND AND AND AND AND AND AND AND AND
V - La l'anglise Acheme
the brivate key of senaci !
of lander for decruption. The algorithm Comment
different signatures, these a signatures are used in the
veufication phase.
Key Greneration:  * The key generation process is same as that of El-Gramo cryptosystem.
exists existing:
sender chaoses prime no. p and primitive 9000 e1.
The completes eg = E, many
bublishes public key = (e1/2) 17 000
the buvale and -4.
L'andina
A TOTAL TIME DATE OF THE STREET
The sender select the nandom number
* The sender select the nandom number 71.  * The sender computes the first signature
* The sender computes the second signature So using the equation: $S_2 = (M-d*X_3)*X_7^{-1} \mod (p-1)$
the equation: So = (M-d * *s) * * T mod (p-1)



### A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science** 



Semester: VI

Subject : CSS

Academic Year: 20 23 20 24

P = large prime number.

M= original message that needs to be signed

sender sends M, S, and S2 to the necesiver.

Step 2: Verifying

The receiver receives M, S, and S2 which can be verified as follows:

\*The neceiver checks to see if 02912p.

\* The neceiver checks to see if 02922p-1.

\* The neceiver performs first past of verification, Viving

the equation: V1 = e, mod p.

\* The neceiver performs second part of verification, V2

wing the equation:  $V_2 = e_2^{S_1} * (S_2)$  mod p

\* If V1 = V2, the signature is valid and the message is accepted, Otherwise, it is rejected.

Example:

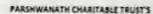
key Generation: -

prime number p=19.

Seled e, = primitive noot of P

Q(p) = (p-1) = (19-1) -18

18 = 2 ×8





## A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science** 



Semester: VL Subject: CSS Academic Year: 2023-2024 Calculate n: = pcp)/pi 18/2 = 9. 18/3 = 6. 2 mod 18 = 8 } 2 is primitive soot. 109 mod 18 = 10 % This is also primitive noot. Inthis case we choose 10. Grad (10,19) = 1 Select d 1 cd < p-2 d=16 .- posivate key. Compute ej: ez = e, a mod p =(10) mod 19. e2 = 4 Publickey = (\$1,e2,p) = (10,4,19) The uses publisheds his public key. Sender hous to generale the signature: Sender X wants to send M=4 to Y. Note: Message M<P. m = H(M) = H(4) = 14 [ Assume that hash function of The Received X should [41 & A westerned ports PARSHWANATH CHARITABLE TRUST'S



# A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering **Data Science** 



Subject: CSS .

Academic Year: 2023 20 24

The sender selects the nandom number (4=5).

Such that gcd ( 5, 91, p-1) = 1. ged (5, 18) = 1.

Compute 8,8 82:-

Si = e, mod p

= 105 mod 19.

81=3

Sa = (M - ds,) r mod (p-1).

\* mod (p-1)

5 mod 18 => 5 # (11) mod 18 = 1.

S2 = 11 (14 - (16)(3)) mod 18.

= 11 (-34) mod 18.

= -374 mod 18.

S2 = 4

The signalure of X & (S,,S2) - The message M=4 & send with signalure S1=3, Sa=4 loy.

The Receiver Y necesives M=4

3,=3

Sa=4.

The Receiver y should verify the signalure. So that he will know that the message is not modified and received from Subject Incharge: Prof. Sarala Mary Page No. 4 Department of CSE-Data Science | APSIT

PARSHWANATH CHARITABLE TRUST'S

# A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering
Data Science



Academic Year: 2023- 20 24

Semester: VI Subject: CSSVeufying: (Receiver Y)  $V_1 = e_1^{M} \mod p$   $V_1 = (10)^{14} \mod 19$   $V_2 = (e_2^{S_1}) (g_1)^{S_2} \mod p$   $= (4)^3 (g_1)^4 \mod 19$   $= 5184 \mod 19$   $= 5184 \mod 19$ 

The signature is valid if V1 = V2.