UNIT 10 *Public Key Cryptography* Overhead Slides

Overhead Slides

OS 10.1 *General Routine*

General Routine	***Example***
1. Choose two prime numbers, p, q	
2. Let $m = p \times q$	
3. Let $A = (p-1) \times (q-1)$	
4. Choose a number E which is less than A and has no factors in common with A.	
5. Find a number D so that $(D \times E) - 1$ is a multiple of A.	

OS 10.2 *Encipher*

$m = 10, \quad E = 3, \quad D = 7$

A	D	E	H	N	O	R	S	T
1	2	3	4	5	6	7	8	9

Message	
Number value	
Power of E	
Value	
Remainder on division by m	

CIPHER message :

OS 10.3 *Decipher*

$m = 10, \quad E = 3, \quad D = 7$

A	D	E	H	N	O	R	S	T
1	2	3	4	5	6	7	8	9

Cipher message	
Power of D	
Value	
Remainder on division by m	
Letter	

MESSAGE :

OS 10.4 *Modulo Division*

Algorithm to find $26^{83} \pmod{115}$

$26^{2} \pmod{115} = \square$

$26^{4} \pmod{115} = \square$

$26^{8} \pmod{115} = \square$

$26^{16} \pmod{115} = \square$

$26^{32} \pmod{115} = \square$

$26^{64} \pmod{115} = \square$

In power of 2,

$83 = 64 + \square + \square + \square$

So

$26^{83} \pmod{115} = \square \times \square \times \square \times \square$

$= \square \bmod 115$

$= \square$