atherin'

1) mathematics of Asymmetric key

of It PS Classifeed Into Six

types they are

of prime Numbers

of primality Testing

of Factorization

of Euler's Theorem

of Chinese Remainder theorem

of Exponentiation and Logorith

prime. Number:

ex An Integer. P71 moral rolls

and p

op If its only diversors of I and P

theorem of arthinetic

## Primality Testing:

A premalety test es an algorithm used for determining white the suput ses prime. It

· A It PS used for cryptography

a premality tests do not generally give prime factors, it States whether the group number PS preme or not

or some primality tests prove that aronumber 95 prome they are

1) The serve of Erothostheres

2) preme factorization

Euler's theorem: can Integer

ap(n) = 1 (mod p) = 2+9 1 1

Consider, a = 3 and n = 10

3 \$(10) = 1 (mod 10)

d(10) = 4

9 811

37 = 1 (mod 10) 2 strt2 scar 81 = 1 (mod 10) of The numbers a and n mist Chinese Remainder theorem: Athe Chinese remainder theorem (CRT) is used to solve a set of different congruent equation with one variable but différent moduli which are relatively prime ( of IFI) 95 a one (of most ruseful results lof & nomber the ory; Consider Some linear system of congruences ison ( in a start (modern)) x = a2 (mod ma) rm n = an (mod nm)

States that the equations ACRT unique Solution of the module a have are relatively prime s that and Eg: the numbers of and x = (a,M,M,-1 agM,M2 ... +anMnMn) mod m Consider a Set of Congurent equation sistementer essents ....  $X = 2 \pmod{3}$ July John July of the source o  $x = 2 \pmod{7}$ 1 = a, (mod m,). x=2 (mod 3) 3 (mod 5) x= az (mod ma) 2 = 2 (mod 7) x= a3 (mod m3) 1. 10 of 100 for mostation X= (a1 M, M, aa Mame) + a3 M3 M3) Mod M m1=3(21 /074) 2/ x Criver a = 2 aa = 3ma=5 ma=7 hora) ax = x a3=2.

to find. Mil from I a light a sign MI. Ma 1013 1 = 1 10 M2 M3-1 M3 find M= m1 x m2 x M3 M = 3x5x tom= + EM x Ell M=105 DOM 1 = FEMARI To find  $M_1 = \frac{M}{M_1} = \frac{105}{3} = 35$ To find  $Ma = \frac{M}{Ma} = \frac{105}{5} = 21$ To find  $M_3 = \frac{M}{M_3} = \frac{105}{100} = 15$ To find inverse of M M, x M, -1 = 1 mod m, 35 xM,-1 = 1 mod 3 35 x 2 = 1 mod 3

M-1 = 2

Max Ma = 1 Mod ma 21 x M2-1 = 1 mod 5 21 × 1 = 1 Mod 3 ma-1 = 1 M3 x M3 = = I Mod M3 E - I 15 x M3-1 = 1 Mod 720= 11 Is xell = Kimodi 7 boil M3-1 =1 M M = 6M 1014 10T = (2 x 35 x2 + 3x21x1 +2x5x1) Mod = 233 Mod 105 inverse. If 7=23/1.

2) RSA Algorithm. A The Rivest - Shamiri- Adleman (Rew) powerted that algorithm for converting plaintext to ciphertext! Athen typical seze for nogs. 1024 bits or 309 decemal digits Algorithm. apick two large prime (numbers p and Q. suich that PFq + EninyPhon \* calculate n=pxa a Calculate pln) = (P-1) x (q-1) expices "e" so that Gritte, p(n)]=1 1 L e L Ø(n) a calculate encryption using C=Mel ? modoonn es 11 = MS

C=Melimodonn () | = Ms)

Decryption using

M = cd mod n

SA Algoridan: Eg:(40) (i) P= 1-to mode - desvisi ent worked wines algoration to 11 = 18 e=7 M=8strate() of Hastoich 2) n = Pxq. = 1 icoique estra 0-5 17 × 1/10- 30H decembly x 511 4.2. n = 187 3)·Ø(n) =(p,-1) (951) = 16 x 10.0=160 的是一個·如此一個一個 4) Entryption & colculate n= PXE (1-5) = (me mod n (1-6)= (mil) = (mil) = (mil) = 11 Le 4 (n) 5) Depuption M = Cd mod no M = 11 23 rmodoom 1875 M = ) - 88 m long by = M

3) Diffie Hellman key excharge: 14 mit is an frist published public Key algorithm. that defenes public key cryptography. A The main purpose of this algorithm
to enable two in users to securely exchange a key that can be used for encuption of Msges 20 torus (- 15 Joer Apithisis algorithm is limited exchange of Secret Vallies why this is secured down 9 - A AIt is uses and discrete algorithm to avoid forced logarithm A st sus private key inol attalla Key & not exclange publica = Key phon S=2

Alice province fish open left sifting Bob mo 21 H asiito della piroche quib sild ploruse of english of Alice denotes private value of Bob 9, -> denotes esperime number denotes Primitives root-PZZ ercharge of sec A = Pa mod questo 21 2id B=Opbo modsigy 21 IEM being provo of mythrolpo aughterni Alia, de doscu YOUB PAI S=B modq

Repestication repudation - Orner & 179

pitary and the frequency