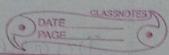
Rivest, Shamis of Ademan ast name of inventors
the oldest (16 year old) public key cryphsystems,
based on difficulty of factoring Each user 1st choosen 2 entremely large knowing the factorisation of n, its easy to compute 4(n) = (P-1) (2-1) e blu I and 40) which is prime to 400 Random number — PA , Ra ZA which has no Common factor with (PA-1)(2A-1) ment A computes nA = PAZA, YNA = NA +1-PA-ZA en modulo your) simultiplicative inverse of this Egn is ; dA = eA' mod (ma) The makes public the anciphering key, and conceals the deciphering key, k(p,A) = (NA)da)

	The Engiphering transformation is Given by:
4/3/78	The same of the sa
	*(P) = PeA mod nA
	deciphering transpormation is given by
23 a	
	f'(C) = CdA mod MA
	terforming & followed by for followed
	Performing & followed by fet or followed by f or followed by fet or fet or followed by fet or followed by fet or followed by fet or fe
44.7	my in order strong throponex is a fee
En 7	10. 1 de
2/1/	We have - N=26 E=3 P=4
	ie., Plaintent consists q toigraphs cirphentent consists q four-graphs in usual 26-letter apphabet.
	caphentent consists of four-graphs.
	In osval 26-letter afphabet.
	lo send Message + 9ts' to a user
	To send Message + 'YEs' to a user with enciphering teys (ma, en) = (46927, 39423)
7	1st her find numerical Equivalent
	YES = 24x(26)2 + 4,(26) + 18x(26)0
	= 16346
	of proposed simple of the solution of the
	the know,
	f(p) = pen mod nA
1 26 41	
	= (16346) 39423 mod 46927
	= 21166



 $= \frac{1 \times (26)^{3} + 5 \cdot (26)^{2} + 8 \cdot (26) + 2}{1 \times (26)^{2} + 5 \cdot (26)^{2} + 8 \cdot (26) + 2}$

the recipient A knows the deciphering key (Donto)

so computes so, for(c) = commod na = (21166) 21767 mod 46927

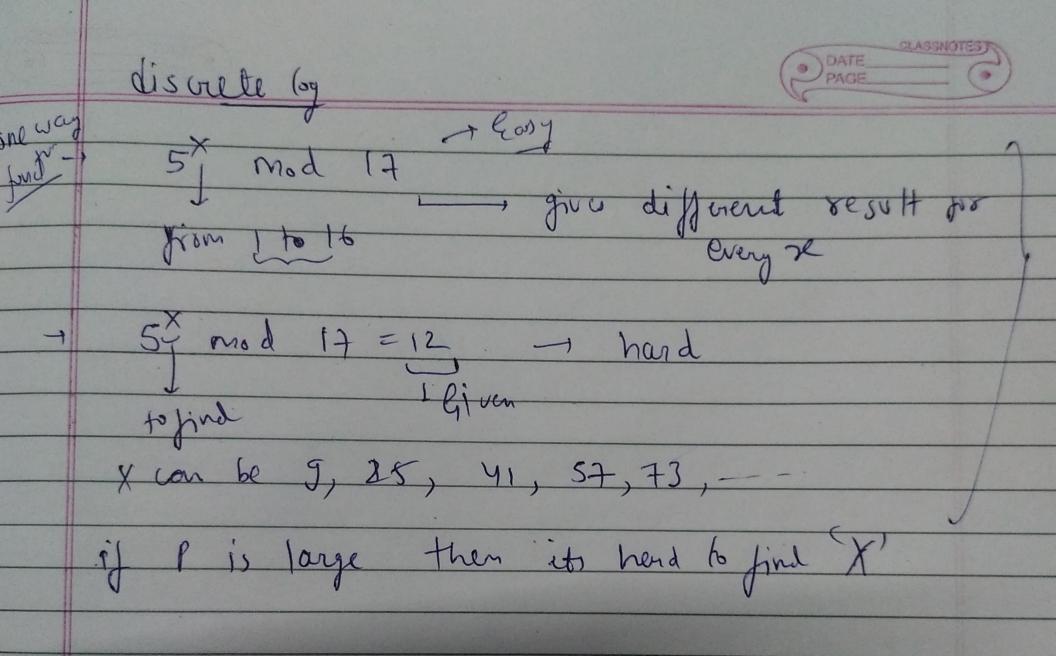
= 16346 = "YES"

how did over A generate her keps?

to get nA, then shooses la at grandom

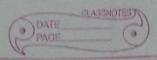
then she found dA = eA' mod 280. 166

numbers PA, 9A, dA remain sevret.



Discrete 109 - If the Gris a finite Group, bes an element in to and y is an element of to which is a power of b then discrete logarithm of y to the base to b is any integer on such that b"=y.

Diffie - hellman key erchange system: In particular, process of aggreeing of on a tey for classical cayptosystem can be accomplished fairly efficiently using a public key system. fisst proposel for doing this was based on discrete logerithmic problem. Matrix transformation of pairs of diagraphs CE (ab) P+(e) mod N' 0 = 9,6, c, d, e, f < N2 where column vector consist of numerical Equi. P is plaintent diagraphs. 7 2 6 and N12, hel com fare - taking nteger k 0,6,c,d,e,f b/w 6 digit ink written to to be base N2.



Jenerating a random element of large finite field Suppose I is public knowledge: everyone knows what finite field has our key will doe in.

- Suppose I is some fixed element of FI, which is also not kept secret. I Suppose that 2 Users A and B want element g Fgt. - which they will we to encrypt their subsequent message to one omother. - A chooses an random integer a b/c 1-42-1.

which she kept secret.

computer ga E F2, - Public Similarly B choose be and Secret key they use is the A gab

tin A trow go (Public key) and A also know
her tray a secret a. so she can
compute gas but a third party
sam only know ga & gb

encryption of single-letter nosssage unit in26-letter alphabet, C=P+Bmod 26. let g be = 2. Suppose A Unoosed a = 2929 and

B has public $\rightarrow 2^b = 12$ then A can complete as (26) a =(12) 29 = 21 FF Meanwhile for A -1229 = 45 is public, then B coan compute as (2ª) b (45) I this Enamples & illustrates mechanics of Diffic Hellman key exchange system.