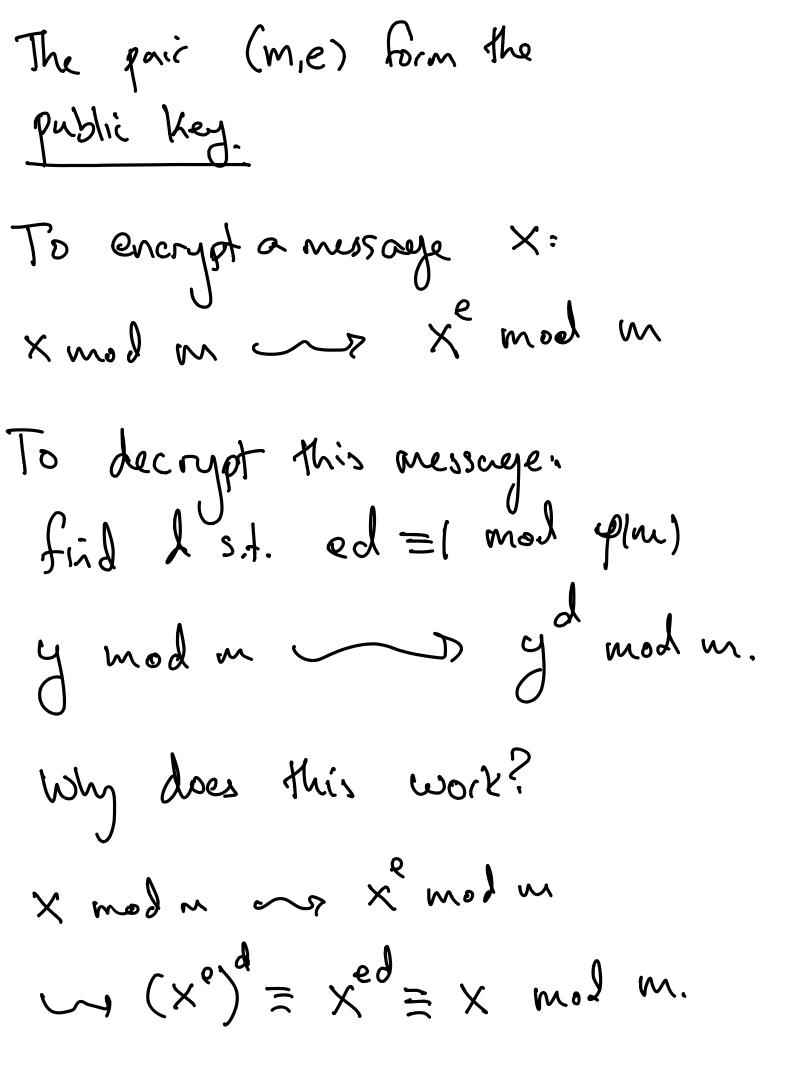
Cryptography
Yesterday: RSA.
How does RSA work?
Bassed off of being able to
Congute roots mod m.
i.e.
$$\chi^{X} \equiv b \mod m$$
 for X.
DSA relies of factoring being hard.
• Bick two large primes p.g. (private)
 $m = pg$.
• Choose $e \in \mathbb{Z}$ w/ $(e, \varphi(m)) = 1$.
 e is called the encryption key



RSA is only secure when d is unknown! In practice, this means when (p(m) is hand to compute. Au example. Use a Substitution Cipher: ß A Space -... Z 02 26 01 27 "MATH IS FUN" 130120072709/192706/2114

M = 1223.2309 = 2823907e = 3 Public Key is (2823907,3). m has 7 dryits, So break our message up uts blacks of at most 6 dryits. Messnye: (130120,072709,192706,Z114) Now encrypt: 130120 mod 2823907 = 1645568 0007 072701 mol -- = 1228979

192706 mod --- = 1307269 2114³ mod ... = 1488629 (1665568,1728979,1307269,6488629) Encryptel message EX: Now Suppose we recrene the following mossage: (1596211,7772934,2761338,787573, 1500275, G37504, 193841) Public per same as before.

We know m=1223.2309 $\varphi(m) = 2820376$ To find d, Solve ed = 1 mod y(m) $3d \equiv 1 \mod 2820376.$ d= 1880257 mod 2820376

 $\lambda = 1880251.$

To decrypt: raise each black to d'mod m: e.g.

1880251 1596211 mod 2823907 = 172101. Do this for each black. Decsypted message: (172101, 180114, 200914, 52709, 192702, 151809, 1407) Use appreto translate back to text: " PLARANTINE IS DORENG!

For a quantum Computer, Kneis an efficient. factoring algorithm Called Shor's algorithm, malaes RSA Derry to Grack. Davadeur, man modern wetholds rely on discrete by problem. (e.g. Elliptic come cryptography)

Discrete loy Powers: XEED mod m

Exponential: $\alpha = 6 \mod m$

When docs a Solution to

ax=6 mod un exist?

A: (for ma prim) Always! Why?

Thum. For an odd prime p there is a number of s.f. $Ord_p(q) = p-1.$ F.e. g?-1 = (modp and gr Z I mod p her

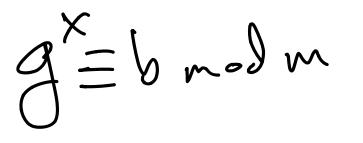
1 < Y < p-Z,

Proof in techne at some point in the future (?).

In particular, the then says

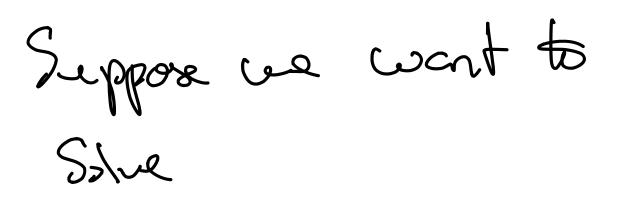
g, g²,..., g^{p-z}, g^{p-1} mod p are all distinct. Mod g thread per non-zero through, So this hits all of them. Thus, For any b, $g^{k} \equiv b \mod m$ der some K. RZE b modern. $\alpha = g^{k}$ $g^{\kappa \kappa} \equiv b \mod m$. So only need to solve for base g.

A number og S.t. Ordp(og) = p-1 R called a generator mod p.



 $'' X = \log_q(b)''$

Example



2^K = 50 mod 101. Fact: Zina generator mod 101.

i.e. $Ord_{loc}(2) = 100.$ $100 = 4.25 \le 2^2 \cdot 5^2$ Idea: work mod 4,25 and que w/ CRT. Let's start mod Z: K=0 mod 2 or K=1 mod 2 X= 22 If $Z^{k} \equiv Z^{2} \equiv 50 \mod 10($ $\implies Z^{lool} \equiv (Z^{lood})^{2} \equiv ($

 $=) 50^{50} = 1 \mod 101$ $=) \in (50^{50} \equiv -1 \mod (01))$ So KEI mod Z. Now work mod 4, K=l+22 and D is even ar old, So KElmoly or KEZmoly Suppose K=3 mod 4. K = 3 + 42 $2 \cdot 2^{\kappa} = 2^{\kappa + 1} = 2^{\kappa + 1}$

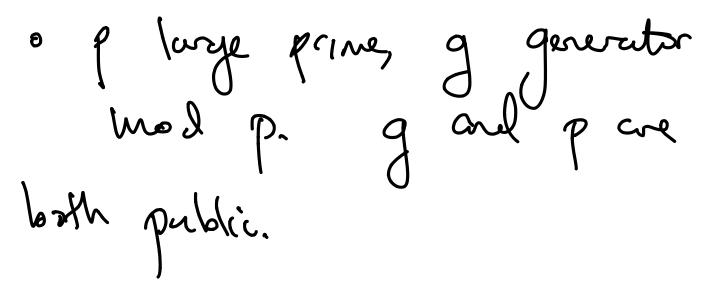
 $\implies (2 \cdot 2^k)^{25} \cong \mathbb{P} \cong [\text{ mod}[0]$ $\implies (2.50)^{25} \equiv 1 \mod 101$ $\left((2.50)^{25} \equiv -1 \mod 101 \right)$ K=3 mod 4. Now work mod S: KEO mol 5 K=5l => 50 =1 =>= mod 5 K=1+52 = (21:50)=1=)= K=1 K=Z mod5 K=ZrSl ⇒ (2?50) =1 ⇒€ $molf x = 3+5l \implies (2.50)^2 = (=) \in$ K=3

KZY mods K=4+5R So $K \equiv 4 \mod 5$ mod 25: l = 0, 1, 2, 3, cf mol 52=4+62 $K = (4, 9, 14, 19, 24 \mod 25.$ A skindes argument shows K= Z4 mol 25. $K \equiv 49 \text{ mel lod}$ $\begin{cases} K \equiv 1 \mod 4 \\ K \equiv 24 \mod 25 \end{cases}$

 $5.2^{49} \equiv 50 \text{ mol } [00.$ Pointi Discrete log is HARD.

How does this apply to Cryptography? Creating encryption Keys!

Diffie -Hellman Create a private they in a public communication Channel.



Alice and Bob want to create
 a Secret key that only they
 will know.

1525p-2 Alue: a Private Bob 6: 6 Keys 1 sp sp-z

Alice computes $A \equiv g^{r}$ and p Bob computes $B \equiv g^b \mod p$ A oul B one their public lings.

Alie and Bob (now both Compute $A^b \equiv B^a \equiv g^{ab} \mod p.$ Z = g^{ab}modq is their Shored pructe Key.

An eausdropper will only know Pigigi, gi. Finding gab modp is the Disarcte log postlen, Sois hardto crack.

Alice and Bobs can now use their Shared private they to set up on appropriate method (e.g. AES).

Ex: p = 101741g= アバテ A= 10947 Allce: a = 52360 B = 56997 5=66235 Bob:

Z = 54692. this is their Key to use his energenon.