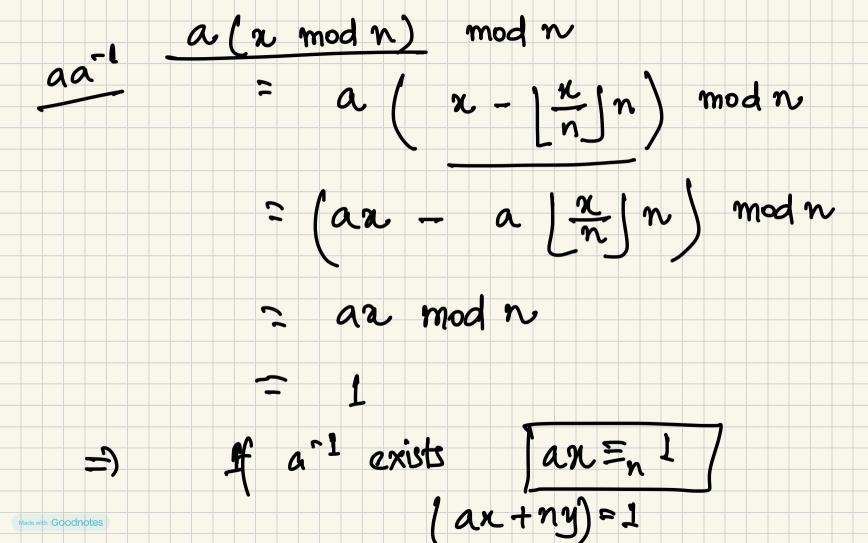
Lecture 19 ACOL 202 det n72 and a e Zn. Then a exists iff a and n are relatively prime. (Contradiction) a = exists => a and n are relatively prime an+ny=1 $-\int a\chi \equiv_n 1$ Made with Goodnotes



If p is prime, every Corollary non-zero a & Zp has a multiplicative inverse. inverse (a, n) where a E Zh, n > 2 = Extended - Enclid x, y, dthen return remod n if d=! " there is no) थडट

Made with Goodnotes

demma {1,2,3,...,}-1} and \$ 19,20, ..., (p-1) a 3 are equivalent mod p where p is prime, a \(\mathbb{Z}_{b}, a \neq 0. Consider the set (\$1ª, 2a, ..., (b-1)a?) - I. All its elements are distinct. None of its elements is zero. 2.

Made with Goodnotes

Does this give us a primality text? If $(a^{n-1} \equiv_n 1)$ for every $a \in \mathbb{Z}_n$ where gcd(a,n) = 1),then does this mean that is prime? But 561 is not ged(a, 541) = 1But 561 is not $a \neq b$ prime. Answer No.

r Eve (eavedropper) Cryptography sccret Bob Alice decryff(c)=m mescage (m) enery bti (plaintact) (cyphentext) Send U Necessary proporties Bob should be able to get m.

Eve should not be able to decrypt (c) ser m.

A simple idea Suppose that Alice and Bob decide

the length of the

message they

would like to

communicate -> M [Suppose they also agree on a secret bitstring K. E. [0,13° where each bitstring is chosen iarependently and uniformly so have on equal since of being choson as K).

Alice encrybt a bitwise XOR 1 KOO) & b and bihaise 10111000 Made with Goodnotes

Eve cannot figure out m by knowing Any m can lead to the same choice of R. 1010110 m: 10101011 K = 0111 Decryption works Encryption works Made with Goodnotes

How do they share the secret key Reusing the same secret key

can make the

protocol insecure. Public - Key Coyptography public key Every participant has a and a private key 1) related

for the publicacy).

Bob Bob decrypts c Sends C (to broduce C) Eve cannot decrypt c

because the private key

is needed for

decryption).

Alice -> Bob (bublic key, primete key) Here is what Bob does:
use two prime nox. N = > 9 Bob chooses e (71) such that e and (p-1).(2-1) are relatively prime. 4. Bob computes d = e modulo (p-1)(q-1) 5. Bob publishes $\langle e, n \rangle$ as his public key

Encryption $m \in \{0, \ldots, n_{Bob}\}$ [c] = m Bob mod w Bob [m]= cdBob mod n Bob Decryptions Suppose Bob picks p= 13
2=17 Example n = 13x17 = 221 $e(\pm 1)$ which is relatively prime to 12x16 e = 5Made with Goodnotes

inverse (5,192) Extended-Euclid (5, 192) Public rey Alice wants to seno m=202 Bob. Made with Goodnotes

mod 221 202 Affice sends to Dob. m = 1206 mod 221This should evaluate to 202. Let us see if it really does. We will use the following facts for the simplification. 1. ab mod K = [(amod K).(bmod K)] mod K 2. ab mod K = [(amod K)b] mod K

= [206 (16 [35 (1204 mod 221) mod 221] mod 221)] = [206 (16 [35 (120) mod 221] mod 221] mod 221 = [206 (16 [1] mod 221)] mod 221 = [206 (16)] mod 221 = 3296 mod 221 = 202. Exercise suppose p=11, 9=13 are the primes chosen by Bob. Further, suppose that he chases the smallest e bissor than I that satisfies the condition necessary for choice of e (that e is relatively frome to (p-1)(q-1)), and publishes his bublic key as (e,1) where m is by. what appearent would you send to 80b if you wanted to send him the plaintext message 95?