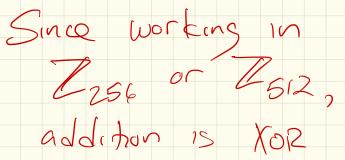


Asymmetric Encryption

Today - Posted , ssue of HW: #1: use all 3 types #2: If no soln, tell ne why - HW due Friday

Last time

AES : (also a bunch of Zn)



Weatness: Need a common key (secret)

More interesting: How do we agree on a secret key.

Best way: Physically exchange

However, impractical for things like web traffic or emails

Public Key Cryptography:

Encryption function E, decryption D

Goals: $\frac{\Delta G}{D} \left(E(M) \right) = M$ (and E(D(M)) = M) E + Dare fast
Given E, hard to derive D

Diffie-Hellman Key exchange From "New directions in cryptography" by Diffie + Hellman in 1976 Daily conspiracy tid bit: Actually discovered by UK government in 1973. Key exchanger' -Start with Zp (p prime or pouer of a prime) These groups have multiplicative inverses: $1.e. \quad 2x = 1 \mod 5$ X=3 15 Inverse

The protocol: Alice + Bob: · p + S<prare both public · Alice chooses secret a < p · Alice posts A=s^a mod p Bob posts B=s^b mod p Alice computes: K= Bª mod P Bob computes: K=Ab modp $B^{a} = (S^{b})^{a} (z = S^{a})^{a}$ $A^{b} = (S^{a})^{a} (z = S^{a})^{a}$

Example: · 5=2, p=29 · Alice picks a=3 Bob picts b=7 X= 23 mod 29 = 8 & Alice Sends B=27 mod 29 = 12 the Bob Sends 8 mod 29 12 mod 29 12 mod 29

hhy? Common tey is k=sab mod p Public info: p, s, A= sa mod p and B= sb mod p What can an attacker try? $A \cdot B = (S^{a})(S^{b})$ $= S^{a+b} X$ Attacker must find. "hidden" exponent.

Hardness?

At its root, the key to why this is difficult is the discrete log problem:

Remember logarithms? 10910 1000 = log_2 1024 =

Hose, discrete vorsion:

Guen A, find logs A = logs St modulo P

How hard? This problem is connected to factoring Lo NOT NP-Hard! But no efficient algorithms are known.

Other tay exchange algorithms work in other groups (like elliptic curves)

RSA: Rivest, Shamir & Adleman Its hardness is tied to > any fast algorithm to factor a number would break RSA.

First: more number theory!

Euler's totient function, P(n): ∮(n):= # of positive integers ≤n that are
relatively prome to n. T T 1.5.7.11 $E_{X} = \overline{\Phi}(12) = \overline{\Phi}'4$ If p rs prime: $<math>\overline{\Phi}(p)=1$ $\overline{\Phi}(7)=1$

What about non-primes? Interesting special case when <u>n= P9</u> p+ 9 prime What is not relatively prime with n? divisors: P+2, 9. P 2p, 3p, -, 9. P 22, 32, ..., 9. P \$(p_2)= ..., 9. P So P2-P-(2-1) $\cdots = (q-1)(p-1)$

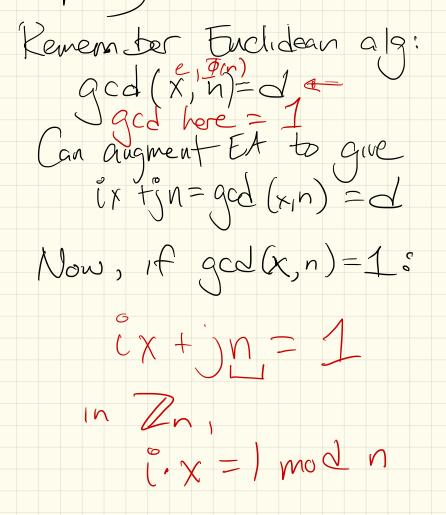
Why we care: Remember, a number E has to be relatively prime to n in order to have a multaplicative inverse in Zn. <u>bx</u>: 5 in Z22 5.9--45 = (imod 22 Vill (9 15 5's inverse Euler's Thm: nEZ, and $x \in \mathbb{Z}_n$ s.t. gcd(x,n) = 1. Then $X^{\overline{\Phi}(n)} \equiv 1 \mod n$.



To compute inverses, need -gcd algorithm & - I(n) Then Euler's thm: $\chi \overline{D}(n) \equiv 1 \mod n$ $\implies X \circ \left(X \stackrel{\overline{\Phi}(n)-1}{\longrightarrow} \right) = 1 \mod n$ More generally, inverses in Zn are a bit more complex...

Back to RSA (ie why we care!) Steps: Select 2 large primes prg ·Let n= pg (p-1)(g-1) · Select e + d s.t. - e and $\Phi(n)$ are relatively prime - ed = 1 mod $\overline{\Phi}(n)$ How to get 2?

Computing inverses:



Extended Euclidean Algorithm:

Euclidean algorithm computed: d = gcd(a,b) by doing gcd(a,b) = gcd(b, a mod b)Let $r = a \mod b$ $\Rightarrow a = bg + r$ for some $g \in \mathbb{Z}$ We will modify Euc Alg So that each call returns not just the gcd, but also i ty also i J where d= i.b t jor 1 inverse wod b

Some ugly math: Goal : $\frac{d}{dnd} r = a \mod b$ and a = gb + r= r = a - gb $\begin{aligned} Tf d &= ib + jr \\ &= ib + j(a - qb) \end{aligned}$ =(J)a+(i-q)b Gy here is a's inverse mod b.

Extended Enc Alg (a,b): If b = 0 (a, 1, 0) $3a = 1 \cdot q + 0 \cdot b$ reduce (a, 1, 0) $3a = 1 \cdot q + 0 \cdot b$ else Trta mod b $(a, i, j) \leftarrow$ Extended Euc Alg (b, r)return $(d, j, \tilde{i} - \tilde{j}q)$ Kuntme. O(log n)

So: RSA (finally!) Bob: Selects 2 large primes prg $\begin{array}{c} \hline & \mathcal{Let} & n = p_{q} \\ & \mathcal{J} & \mathcal{J}(n) = (p-1)(q-1) \end{array}$ · Select e + d s.t. - e and $\Phi(n)$ are relatively prime - $ed \equiv 1 \mod \overline{\Phi}(n)$ Now: (e,n) is public by • d is private tey (also p 9 9)

Encryting: Alice gets (e,n).

She takes a message M, with O < M < n. (chops into pieces)

Then: Ca Me mod n

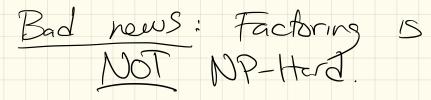
(Remember public part: (E,n) was teg)

Alice Sends C to Bob

Decrypting: Bob gets C C= Me mod n Bob Calculate: Claim: M Why? C mod n = (M^e)^d mod n = Med mod n Ynow $ed = 1 \mod \widehat{\Phi}(n)$ Med = M(ED(n)+1) mod h = (M (m) ~ Minod n = 1 ~ Minod n = M

<u>So</u>: Why secure? Bob can decrypt! He berows (secret) d. Attacher Eve's goal: Figure out d! How ? " Bob needed \$(n), since d is e's inverse mod n. •Attacker knows n(but not $\overline{\mathcal{P}}(n)$). How to find $\overline{\Phi}(n)$?





Best aborithm: Number field sieve: O(e⁴⁴ logn)³ (log logn)^{2/3})

Some practical notes - RSA can be used to encrypt entire message (but usually Isrit) - Slow (compared to XOR-ing) - Easier to break than AES or other symmetric protocols - Also: I was assuming (M,n) = 1Here, saved since n=pg, VM will be relatively prime to porg.