CIS 3362 11/2/2022

Record Quiz 4 Review Tonight 8-9pm (hope)

Aids

1 sheet notes (8.5" x 11") you bring

Calculator

Date: 11/9 12:30pm

Don't meet in person Monday 11/7 (Watch recording instead!)

Today: RSA encryption

Ron Rivest
Adi Shamir
Leonard Adleman
] Interested in creating public key crypto system

General set-up: Some public info posted by Alice Alice's Public Keys. She also has corresponding Private Keys, but knowledge of Public Keys don't reveal info about private keys.

Allows others to send encrypted messages to Alice knowing that only Alice should be able to decrypt the message.

Private keys: 2 large primes P, Q (Alice picks)

Public key #1: $n = PQ$

Private info/key: $\phi(n) = (P-1)(Q-1)$

~~Next~~

Public key #2: Choose e, such that $\gcd(e, \phi(n)) = 1$.

Next Private key: $d = e^{-1} \bmod \phi(n)$

Public keys: n, e

Private keys: P, Q, d, [$\phi(n)$ should be kept secret]

Bob to send MSG to Alice, M,
$0 \leq M < n$

$C = E(M) = M^e \bmod n$ (encryption)

Alice $D(C) = C^d \equiv M \bmod n$

$C^d = (M^e)^d$

$= M^{ed}$

$= M^{k\phi(n)+1}$

$= M^{\phi(n)k} \times M^1$

$= (M^{\phi(n)})^k \times M$

$\equiv 1^k \times M \bmod n$, via Euler's Thm, assuming $\gcd(M, n) = 1$

$d = e^{-1} \bmod \phi(n)$

$\Rightarrow ed \equiv 1 \bmod \phi(n)$

$ed = k\phi(n) + 1$ for some int k.

How do I convert text to a number and vice versa?

(1) Base 26 use only letters

$COMPUTER = 2\times26^7 + 14\times26^6 + 12\times26^5 + 15\times26^4 + 20\times26^3 + 19\times26^2 + 4\times26^1 + 17\times26^0$

Find max of k such that $26^k < n$.
Make the input into blocks of k characters.

* Ciphertext remains in numbers.

(2) Radix 64 (encodes upto 64 chars, letter lower, upper, digits, +, −)

(3) Store data in byts. Figure out max k s.t. $256^k < n$. Store k bytes in a single int.

```
  0 1 2                i   val = 0          C
  C A T                0   val = 26*val + 2  = 2
    ↑                  1   val = 26*val + 0  = 52
    C
```

(26*val: shifts left all old values; 0: new val)

$606 = 2$
1352
19

```
  ← CA ↑               2   val = 26*val + 19 = 1371
```