CIS 3362 10/29/21

RSA

(1) Pick large primes p, q (private key)

(2) Calc $n = p \cdot q$ (public)

(3) Pick e, s.t. $\gcd(e, \phi(n)) = 1$
$\phi(n) = (p-1)(q-1)$. (public key)

(4) Calc $d \equiv e^{-1} \bmod \phi(n)$ (private key)

Send me a msg:

$C \equiv M^e \bmod n$

Decrypt

$C^d \equiv M \bmod n$

$C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{k\phi(n)+1}$, since $ed \equiv 1 \bmod \phi(n)$

$\equiv M^{k\phi(n)} \cdot M^1 \equiv (M^{\phi(n)})^k \cdot M^1$, $\gcd(M, n) = 1$

$\equiv 1^k \cdot M \equiv M \pmod n$

Question

How do I encode msg as #?

(1) Bits (ascii, etc.)

(2) Break into blocks n 100 bits

Uppercase letters $A=0, B=1, \ldots Z=25$

"CAT" $= 2 \times 26^2 + 0 \times 26^1 + 19 \times 26^0$

figure out max letters in a block

Radix-64 Encoding (lower, upper, digits, -, +)