

Math 321

Q's / 3.6 #27

$$1 = a_k z^k + a_{k-1} z^{k-1} + \dots + a_2 z^2 + a_1 z + a_0$$

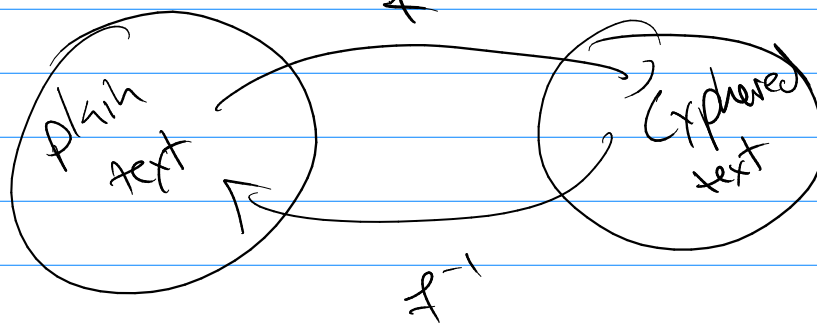
$11 \approx 1$

$$a_i \in \{0, 1\}$$

use $11 \approx 1$ but $b=2$

3.7 Crypto.

Private vs Public.



Private: f^{-1} is easy to find given f .


Q Caesar Shift. Alphabet = A \wedge $|A| = n$

② English $|A| = 26$

$$f(p) = (p + K) \bmod 26$$

A B C ... Z let $K = 3$
" " " " " " " "
0 1 2 25

z A B C $f(C) = f(2) = (2 + 3) \bmod 26 = 5 = E$


$$f^{-1}(p) = (p - K) \bmod 26$$

$$f(p) = (p + K) \bmod n$$

$$f^{-1}(p) = (p - K) \bmod n$$

$$|A| = n$$

One-time-pad.

Caesar shift
+K

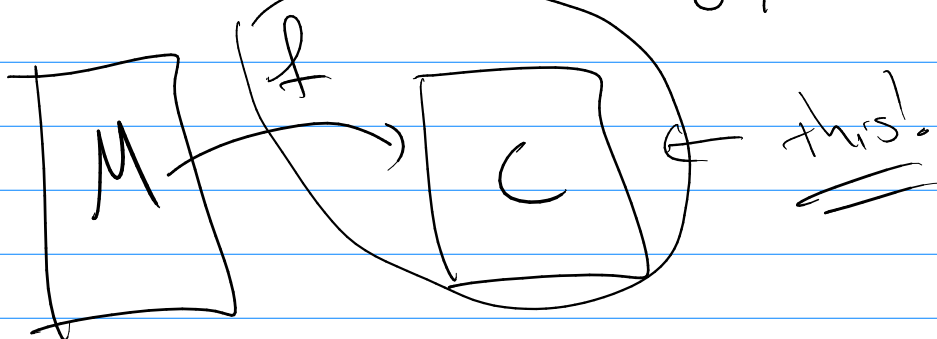
	MARK	WAS	HERE
⊕	↓↓↓	↓↓↓	↓↓↓
	NBSL	XBT	IFSF

One-time
pad

MARK WAS HERE
 $\downarrow \downarrow \downarrow \downarrow \quad \downarrow \downarrow \downarrow \quad \downarrow \downarrow \downarrow \downarrow$
 $\rightarrow \begin{array}{|c|} \hline +1 +2 +3 \\ \hline \end{array}$
 $\downarrow \downarrow \downarrow$
 $N N N$

Public:

What do the "bad guys" know.



Public means given f , then f^{-1} is
"probably" "hard" to find.

What is needed?

① Bézout's Identity

$$\gcd(a, b) = s \cdot a + t \cdot b$$

for some $s, t \in \mathbb{Z}$

(ex) $\gcd(7, 11) = 1$

$$11 = 7 \cdot 1 + 4 \quad \begin{matrix} q_1 \\ r_1 \end{matrix}$$

$$7 = 4 \cdot 1 + 3 \quad \begin{matrix} q_2 \\ r_2 \end{matrix}$$

$$4 = 3 \cdot 1 + 1$$

$$3 = 1 \cdot 3 + 0 \quad \gcd(7, 11)$$

$$1 = 4 - 3 \cdot 1$$

$$1 = 4 - (7 - 4 \cdot 1) = (-1)(7) + (2)(4)$$

$$1 = (-1)(7) + (2)(11 - 7)$$

$$1 = (-3)(7) + (2)(11)$$

$$\uparrow \quad \gcd(7, 11) = 5 \cdot 7 + 6 \cdot 11$$

(2) Identity vs Inverse

$$x + 2 = 4$$

$$x + 2 + (-2) = 4 + (-2)$$

$$x + 0 = 2$$

$$x = 2$$

Modular
Arith

$$3 \equiv_n a$$

$$c \equiv_n d$$

$$3 + c \equiv_n a + d$$

ex $1 \equiv_5 6$ $1 \equiv_5 11$ $1 \equiv_5 16$
 $1 \equiv_5 -4$

so $x \equiv_5 3 \rightarrow x+1 \equiv_5 3+(-4)$

$$\left[\begin{array}{l} a+c \equiv_n b+d \quad a \equiv_n b \quad c \equiv_n d \\ ac \equiv_n bd \end{array} \right]$$

Identity $a \cdot \underbrace{1}_n \equiv a$

Inverse?

$$a \cdot \underbrace{x}_n \equiv 1$$

how to find.

Bézout's Identity.

$$\gcd(a, b) = 1$$

$$1 = s \cdot a + t \cdot b$$

apply mod b

$$1 \pmod b = (s \cdot a) \pmod b + (t \cdot b) \pmod b$$

$$s \cdot a \bmod b = 1$$

↑
a's inverse mod b.

So $a^{-1} \equiv_n 1$ Need $\gcd(a, n) = 1$

use Euclidean Alg. (Extended)

$$1 = \underbrace{(s \cdot a + t \cdot n)}_{\substack{\uparrow \\ \text{a's inv. mod } n}}$$

RSA: $C = M^e \bmod n$

$\hookrightarrow M = C^d \bmod n$

$(M^{e/d}) \bmod n$

Need: $\boxed{e, d, n}$

technique

① Find large primes p, q

② $\underline{n} = p \cdot q \quad M = (p-1)(q-1)$

③ pick e such that

$$\gcd(e, \underline{M}) = 1$$

④ Find d e 's inverse

$$d \cdot e \equiv 1 \pmod{M}$$

$$C = M^e \pmod{n}$$
$$M = C^d \pmod{n}$$