Fermat's Little Theorem

$a^{p-1} \equiv 1 \bmod p$

$a^{p-1} \bmod p = 1 \bmod p = 1$

$7^2 \bmod 3 = 1$

$\frac{49}{3} = 48 \text{ R } 1$

Modular Inverse

$a \bmod m$

$a \cdot x = 1 \bmod m$

a and m coprime

Euler's totient

- number of coprimes to n, less than n

$\varphi(p) = p-1$

$\varphi(n) = \varphi(\text{prime factorization of } n)$

↳ $\varphi(10) = \varphi(2) + \varphi(5)$

$= 1 + 4 = 5$

3, 4, 7, 9

Miller Rabin Alg

- given odd n
- $n-1 = 2^r * d$
- pick a, $2 \le a \le n-2$

repeat:
- $a^d \bmod n = 1$? follow fermat's?
- $a^{2^k * d} \equiv 1 \pmod n$, $0 \le k \le r-1$

- likely if prime
- certain if composite

Stream Cipher

- 1 bit plaintext, 1 bit keystream processed at a time for 1 bit ciphertext
- same for decryption
  - random keystream → unbreakable other than same keystream

Block Cipher

- blocks of size n to produce ciphertext of size n

Symmetric / Substitution ciphers:

- Caesar cipher: shift alphabet
- monoalphabetic: any alphabet permutation
  - ↳ frequency cipher
- playfair cipher
  - plaintext: lord, ciphertext: orda

l	o	c	d	a
b	c	e	f	g
h	i/j	k	m	n
p	q	r	t	u
v	w	x	y	z

lo = or
rd = da
orda

- hill cipher

hi = [7, 8]

h	o	d	3	f
b	l	e	4	h
c	2	f	5	i

$([7,8] \cdot K) \bmod 26 = \text{cipher}$

$(\text{cipher} \cdot K^{-1}) \bmod 26 = [7,8] = hi$

- polyalphabetic cipher

Vigenere

plaintext: iloveyou
key: herbherb
→ ppfwrcfv

	A	B	C	D	E	...
A	a	b	c	d	e	...
B	b	c	d	e	f	...
C	c	d	e	f	g	...
D	d	e	f	g	h	...
E	e	f	g	h	...	
⋮	⋮	⋮	⋮	⋮		

Vernam

plain: 1011
key = 0111

plain ⊕ key = 1100 ciphertext

1100 0111
ciphertext ⊕ key
1011
→ plaintext

one time pad

- use single random key for each message
- no statistical relationship
- secure key distribution difficult

transposition ciphers

- rail fence cipher
  - security at discretion, key: number of rows
  - plaintext: hello what's up

key = 3

h o t
e l w a s p
l h u

↳ hot elwasp lhu

- row transposition

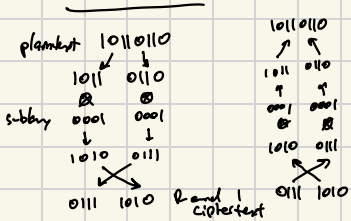
1	2	3	4	5
t	r	a	n	s
p	o	s	i	t
i	o	n	x	x

4 3 1 5 2 → n a t s r / i s p t o / x n i x o

natsrisptoxnixo

4 3 1 5 2
n a t s r
i s p t o
x n i x o

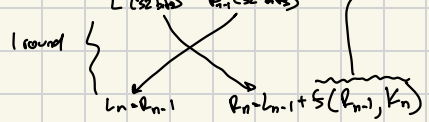
feistel cipher



DES

data: 64 bits
key: 64 bits, only 56 used

1. subkey gen
   - K: 64 bits → permute table → K+: 56 bits
   - C0 D0 → C0D0: 56 bits → 48 bit table permute → K0
   - C1 (shift 1 bit) D1 → C1D1: 56 bits → K1
   - (shift each bit)
   - ⋮
   - → CnDn: 56 bits → Kn
   - C15 D15 → C15D15: 56 bits → K15
2. block encode
   - M: 64 bits
   - → IP permute → M: 64 bits
   - L (32 bits) R (32 bits)



$f(R, K) =$

R: 32 bits
↓ E(R) expansion permutation table
R*: 48 bits

$B(R^*, K) = R^* \otimes K$

↓ break into 8 groups of 6

$S1(B1)S2(B2)\dots S8(B8)$

$S(B)$ = mapping of B

$P[S(B)]$ → permute the groups?

$S(R, K) = P(S(B(E(R) \otimes K)))$

decrypt w/ reverse order

- characteristics
  - S tables have unique nature
  - key size + 16 rounds easily crackable with today's supercomputers

Finite Fields

Group: set with binary operation $*$
- A1: closure under $*$
- A2: association with $*$
- A3: identity element for $*$
- A4: inverse element for $*$

↳ Abelian Group:
- A5: commutative property for $*$

↳ Ring $\{R, +, *\}$
- A1-A5: for addition "+"
- M1: closure under multiplication "*"

↳ Commutative Rings
- M4: Commutativity of multiplication

↳ integral domain
- M5: multiplicative identity
- M6: no zero divisors

↳ Fields
- A1-M6
- M7: multiplicative inverse $a^{-1} \cdot a = 1$

↳ Finite field

GF(p)

ex. $GF(5) = \{0,1,2,3,4\}$

additive inverse:

0	1	2	3	4
0	4	3	2	1

$1+4 \bmod 5 = \emptyset$
$2+3 \bmod 5 = \emptyset$

multiplicative inverse:

1	2	3	4
1	3	2	4

$1 \times 1 \bmod 5 = 1$
$2 \times 3 \bmod 5 = 1$
$4 \times 4 \bmod 5 = 1$

↳ Finite field expansion $GF(p^n)$
- n: order of polynomials
- p: set of prime nums $\{0 \dots p-1\}$
- irreducible polynomial $m(x)$ of degree n

- $GF(2^2) = \{0, 1, x, x+1\}$

$m(x) = x^2$

$x \cdot x \bmod x^2 = \emptyset$
$x+x \bmod 2 = \emptyset$
$x+1-1 = x$