EMAIL → spr@cs.rit.edu

CRYPTO CRASH COURSE

CRYPTO GOALS
- ↳ CONFIDENCIALITY/SECURITY
- ↳ DATA INTEGRITY
- ↳ AUTHENTICATION
- ↳ NON-REPUDIATION

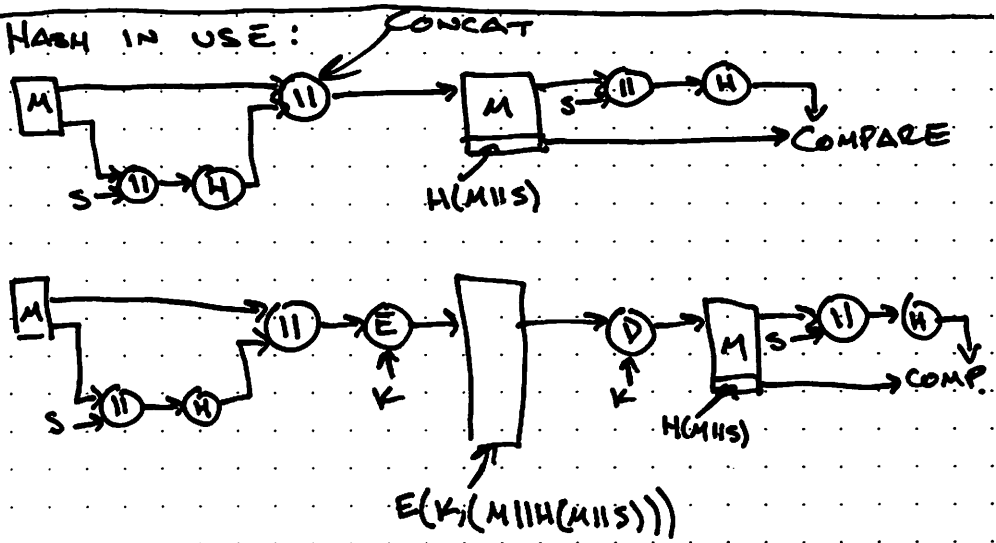
CRYPTO LIMITS
- ↳ RIGHT CHOICE OF TOOLS IS HARD
- ↳ IMPLEMENTATION ERRORS ARE COMMON
- ↳ SIDE-CHANNEL ATTACKS ARE DOPE
- ↳ SOCIAL ATTACKS

PRIMITIVES, ALGORITHMS, [redacted] PROTOCOLS
- ↳ UNKEYED, SYMM. KEYED, PUB.-KEY

UNKEYED:
- ↳ HASHING
- ↳ SHA FAMILY

USE
- ↳ HASH & SIGN
- ↳ RANDOM SEQUENCES
- ↳ MANY OTHERS

HASH IN USE:

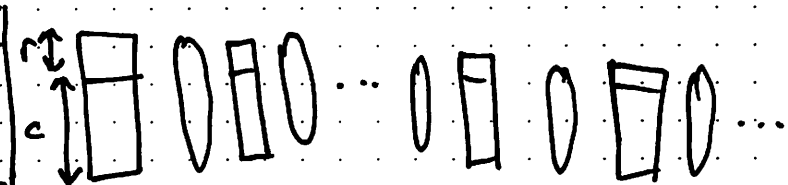


SHA-3:
- ↳ KECCAK 2007-2050?
  - ↳ FIPS 202
- ↳ SPONGE DESIGN
- ↳ RUNS ON A 5×5×2^l CUBE OF BITS, l=6

AES	128	192	256	SEC LEVEL
		↓×2		
SHA3	256	384	512	

(BIRTHDAY PARADOX)

SHA-3/SHAKE/KECCAK SPONGE

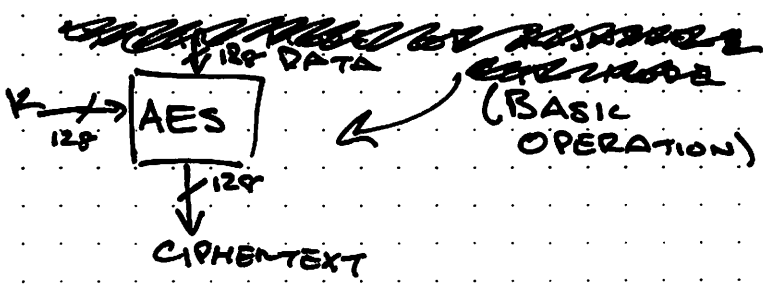


SYMMETRIC KEYS
- ↳ BLOCK CIPHERS SINCE 70'S
  - ↳ IBM LUCIFER
  - ↳ DES
  - ↳ IDEA
  - ↳ AES
- ↳ STREAM CIPHERS, RC4 - ALSO CAN COME FROM COUNTER MODE OF BLOCK CIPHERS
- ↳ MAC, HMAC
  - ↳ MESSAGE AUTH CODES
- ↳ RNG
  - ↳ NOT AS GOOD AS TRNG

DES: [redacted] OBSOLETE & DUMB

AES: WON NIST CIPHER IN 1997-2001
- ↳ NAT. INST. OF STANDARDS [redacted]
- ↳ OH BOY IT USES GF! TECH
- ↳ STATE IS A 4×4 MATRIX IN GF(2^8)

BLOCK CIPHERS



ENCRYPT BLOCK BY BLOCK
↳ DECRYPT BY REPEATING ENCRYPTION

PUBLIC KEY CRYPTO
↳ RSA, ELGAMAL, ECC

↳ SIGNATURES
  ↳ DSS/DSA - DIGITAL SIGNATURE STANDARD & ALGORITHM
  ↳ ECDSA - ELLIPTIC CURVE ...

↳ PKI - PUB. KEY INFRASTRUCTURE
  ↳ NOT GREAT
  ↳ DIFFIE-HELLMAN
↳ HOMOMORPHIC CRYPTO
  ↳ JUST ASK PRATHIBA
  ↳ PERFORM OPS ON ENC. DATA

RSA V. ECC
↳ RSA
  ↳ SIMPLE & WELL DEFINED
  ↳ LINKS NICELY TO # THEORY
  ↳ DEPLOYED EARLIER
↳ ECC
  ↳ SHORT KEYS
  ↳ BETTER PERFORMANCE
  ↳ USES REALLY COOL THEORY

OTHER COMPOSITE & SPECIAL FUNCTIONS
↳ ZERO-KNOWLEDGE PROTOCOLS
↳ AUTHENTICATED ENCRYPTION CAESAR COMPETITION

↳ ELECTRONIC CASH
↳ CRYPTO-CURRENCIES
↳ ELECTRONIC VOTING
↳ OBLIVIOUS TRANSFER, TWO MILLIONAIRES PROBLEM
↳ QUANTUM & POST-QUANTUM CRYPTO

MATH IN CRYPTO

MATH IN PRIMITIVES
- ↳ KEYLESS
  - ↳ MOSTLY JUST BIT-JUGGLING
- ↳ SHARED-KEY
  - ↳ MOSTLY $GF(2^k)$
- ↳ PUBLIC KEY
  - ↳ LOTS OF # THEORY

MATH IN CYRYPTANALYSIS
- ↳ LINEAR & DIFF CRYPTANALYSIS
- ↳ PROB & STATS
  - ↳ RANDOM ORACLE MODEL
- ↳ NUM. THEORY ALG.
  - ↳ PRIMALITY & FACTORING
- ↳ DISCRETE LOGARITHMS

CRYPTOGRAPHY ENGINEERING

SECURITY ENG. MUST CONSIDER
- ↳ LEVEL OF SECURITY
- ↳ FUNCTIONALITY
- ↳ PERFORMANCE
- ↳ SIMPLICITY

$\varphi(n)$, EULER TOTIENT FUNC.

~~$\varphi(n) = \#(\mathbb{Z}_n^* \text{ for } \mathbb{Z}_p)$~~ $\mathbb{Z}_n = \{0, 1, \ldots, n\}$

$\varphi(n) = |\{a : 0 < a < n \wedge \gcd(a, n) = 1\}|$

P - PRIME $(2, 3, 5, 7, 11, \ldots)$

$\mathbb{Z}_n^* = \{a : 0 < a < n \wedge \gcd(a, n) = 1\}$

↑ POSS. REMAINDERS, INVERTIBLE MOD n

HW #2 - MODULO FUNCTION
- ↳ CRYPTOOL - SOFTWARE DEMONSTRATION

GOING OVER CH.1 SLIDES FROM SPRINGER

NT INDUCTION TO COMPUTE φ:

① $n = p \rightarrow n = 3$

$\mathbb{Z}_3 = \{0, 1, 2\}$

$\mathbb{Z}_3^* = \{1, 2\}$

$\varphi(3) = 2$

$n = 4$

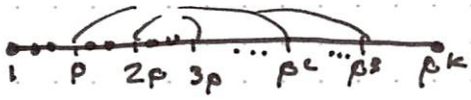
$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$\mathbb{Z}_4^* = \{1, 3\}$

$\varphi(4) = 2$

$\varphi(P) = P - 1$

② $n = p^k \rightarrow$ $\gcd \neq 1$



IS NOT A DIVISOR OF...

$\gcd(a, p^k) = 1$ IFF $p \nmid a$

$\varphi(p^k) = p^k - \frac{p^k}{p}$

$= p^{k-1}(p-1)$

③ $n \cdot m$, $\gcd(n, m) = 1$ (VIA CRT)
- ↳ CHINESE REMAINDER THEOREM

$\varphi(nm) = \varphi(n)\varphi(m)$

MULTIPLICATIVITY

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

$= (1)(4) = 4$

$\varphi(10000000000) = \varphi(10^{10})$

$= \varphi(2^{10})\varphi(5^{10})$

$= 2^9(1) \cdot 5^9(4)$

$= 512 \cdot 5^9(4)$

$4 \cdot 10^9 = 2048 \cdot 5^9$

$\varphi(999) = \varphi(3^3 \cdot 37)$

$= \varphi(3^3)\varphi(37)$

$= 3^2(2) \cdot 36$

$= 9 \cdot 72$

$= 648$

THEOREM: (PROOF LATER) — EULER THRM

IF $\gcd(a,n)=1$ THEN $a^{\varphi(n)} = 1 \bmod n$

$n = 11$: % 11

$a = 3^i$: 0, 3, 9, ~~7~~, 5, 4, (1), 3, 9, 5, 4, 1

$i=0$; $i=10 = \varphi(11)$

ORDER OF $a \bmod n$ (IF DEFINED) IS THE SMALLEST $k>0$ SO $a^k = 1 \bmod n$

$\mathrm{ORD}_n(3) = 5$

$a = 2^i$: ~~1~~, 2, 4, 8, 5, 10, 9, 7, 3, 6, (1)

$i = 10$

~~$\mathrm{ORD}_x(a) = 10$~~

$\mathrm{ORD}_{11}(2) = 10$

LAGRANGE THEOREM:
FOR $\gcd(a,n)=1$
$\mathrm{ORD}_n(a) \mid \varphi(n)$
DIVISOR

DEF: (GENERATOR)
a IS PRIMITIVE IFF
$\mathrm{ORD}_n(a) = \varphi(n)$

THEOREM:
IF THERE IS A PRIMITIVE $a \bmod n$, THEN THERE IS A $\varphi(\varphi(n))$

EXP(mod n), SUSPECTED TO BE ONE-WAY FUNCTION (OWF)

exp: GIVEN x, y, n COMPUTE $z = x^y \bmod n$

DL: DISCRETE LOG
GIVEN x, z, n COMPUTE y

INFEASIBLE ~~IMPOSSIBLE~~ BELIEVED TO BE TO COMPUTE FOR PROPERLY CHOSE $x, n \approx 2^{2048}$

COMPUTING $x^y = x^{[\text{binary } y]} \bmod n$

LOOK @ LSB

ODD VS EVEN

$x^{2k} = (x^k)^2$
$x^{2k+1} = (x^k)^2 \cdot x$
} $\bmod n$

$x^6 = (x^2 \cdot x)^2$
$x^6 = (x^2)^2 \cdot x^2$
} 3 MULTS

$x^{11} = ((x^2)^2 x)^2 x$ — 5 MULTS

$2\log_2(y)$ MULTS

1) EA - EUCLID ALGORITHM
2) EEA - EXTENDED EA

1. GET $\gcd(a,b)$
2. IF ~~d~~ $d = \gcd(a,b) = 1$ then get $a^{-1} \bmod b$, $b^{-1} \bmod a$

EEA FINDS x, y SO $d = xa + yb$ → $d=1$ → $y = b^{-1} \bmod a$; $x = a^{-1} \bmod b$

EA: GCD(a, b):
IF $b=0$ RETURN a
ELSE RETURN GCD$(b, a \bmod b)$

EUCLID: RETURNS TRIPLE (d, x, y)

$d = \gcd(a, b) = xa + yb$

IF $b = 0$
RETURN $(a, 1, 0)$

RECURSIVE CASE REQUIRES THAT:
$a = qb + r$
& $d = x'b + y'r$

$d = x'b + y'(a - qb) = y'a + (x' - qy')b$

$(d, x', y') \leftarrow \gcd(b, a \bmod b)$
$(d, x, y) \leftarrow (d, y', x' - y'\lfloor a/b \rfloor)$
RETURN (d, x, y)

EX: $d = 1$

a	b	q	r	x	y	x'	y'
31	5	6	1	1	-6	0	1
5	1	5	0	0	1	1	0
d → 1	0						

RESULT: $1 = 1 \cdot 31 + (-6)5$

$1 = 31^{-1} \bmod 5$

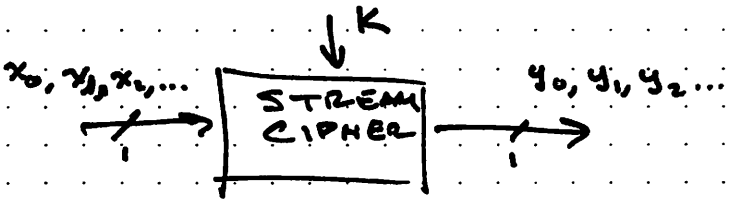
$-6 = 25 = 5^{-1} \bmod 31$

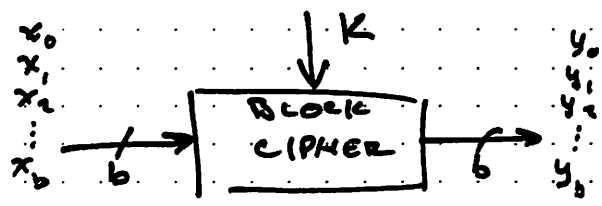
EX:

a	b	q	r	x	y	x'	y'
29	17	1	12	-7	12	5	-7
17	12	1	5	5	-7	-2	5
12	5	2	2	-2	5	1	-2
5	2	2	1	1	-2	0	1
2	1	2	0	0	1	1	0
d = 1	0						

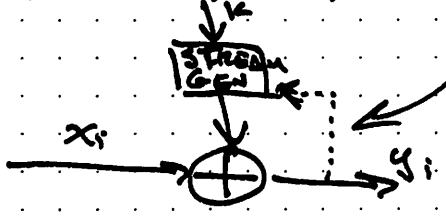
RESULT: $1 = -7(29) + (+12)(17)$

STREAM CIPHERS





SYNC VS. ASYNC STREAM CIPHER



OTP/PRNG/STREAM CIPHERS

↳ ENC. $e_{k_i}(x_i) = x_i \oplus k_i$

$d_{k_i}(y_i) = y_i \oplus k_i$

RNG MADE OF PUFS ?

LINEAR CONGRUENTIAL GENERATOR

↳ CHECK NOTES

↳ LFSR IS A REFINEMENT

FAST & UNIFORM

RSA GEN

↳ NOTES FOR ALG.

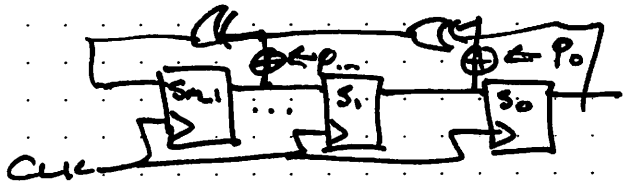
↳ SLOW / UNPREDICTABLE

BLUM-BLUM-SHUB

↳ NOTES FOR ALG.

↳ CLAM: CAN USE (LOG (LOG n)) BITS PER ITERATION

LFSR



$s_i \ldots s_1 s_0$

2^m CONFIGURATIONS

m: # OF FFS

MAX OUTPUT LEN: $2^m - 1$

PARALLEL LOAD ALL 0's

LFSR SECURITY

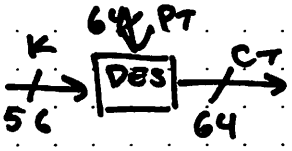
$P(x) = x^m + p_{n-1}x^{m-1} + \ldots + p_1 x + p_0$

HIGHLY PREDICTABLE OUTPUT

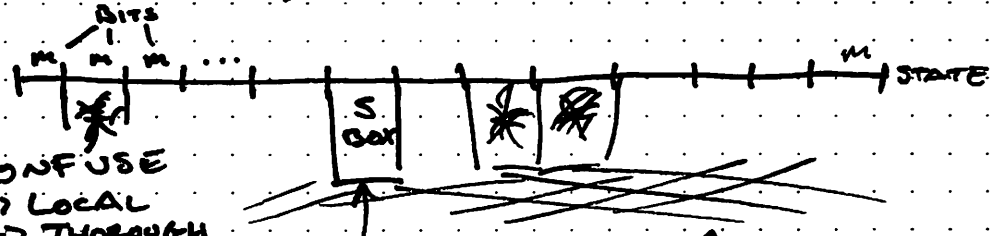
EXAM - CC:
- ↳ CH 1, 2, 3
- ↳ CONTENTS OF HANDOUTS, HMWKS, NOTES
- ↳ 1-SIDED CHEATSHEET
- ↳ INCLUDES DES STUFF

DES:

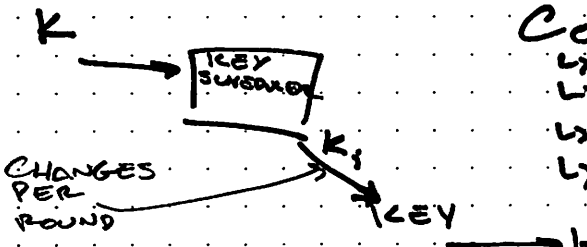
↳ SYMMETRIC KEY BLOCK CIPHER



SPN: SUBSTITUTION-PERMUTATION NETWORK



CONFUSE
- ↳ LOCAL
- ↳ THOROUGH
- ↳ DO TO m-BIT CHUNKS
- ↳ NON-LINEAR



DIFFUSION
- ↳ MOVES CHUNKS AROUND STATE
- ↳ LINEAR
  - ↳ USUALLY
- ↳ BROAD
- ↳ SIMPLE

CONFUSE, DIFFUSE, KEY

ROUND

ROUNDS

ITERATE

DES: 16 ROUNDS

AES: 10
12 ROUNDS
14

DEP. ON STRENGTH

DES CRACKED IN LATE 90's BY EXHAUSTIVE ENUM OF KEYS
- ↳ 2DES DIDN'T WORK
- ↳ 3DES IS STILL USED TODAY
- ↳ REPLACED BY AES

DES USES A FEISTEL NETWORK
- ↳ ENCRYPTION & DECRYPTION ARE "THE SAME"

RUN BACKWARDS FOR DECRYPT

REARRANGE

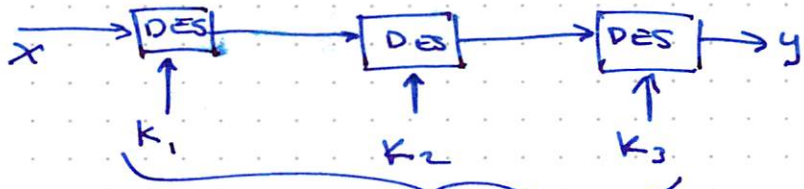
$$\text{ENC}\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \end{cases} \qquad \text{DEC}\begin{cases} L_{i-1} = R_i \oplus f(L_i, K_i) \\ R_{i-1} = L_i \end{cases}$$

HW TO PRACTICE FOR EXAM – LFSR & DES ! GRADED
↳ CH 1, 2, 3
↳ EXTRA POSTINGS UNTIL DESPLUS

EXAM ALLOWS 1 PAGE OF NOTES
~~↳ CONTENT~~ ↳ CAN BE TYPED
↳ COULD BE A FUN LaTeX GAME...

- KNOW FEISTEL CIPER
- DES, ~~2DES~~, 3DES

3DES



CAN BE (DON'T NEED TO BE) DIFFERENT KEYS

$$y = DES_{K_3}(DES^{-1}_{K_2}(DES_{K_1}(x)))$$

↑ DECRYPTION IN MIDDLE

NON-LINEAR

S-BOX SIZES THROUGOUT HISTORY:
↳ SIMPLE DESIGNS 4-4
↳ SERPENT 8 BOXES
DES (8) 4x16x8x4 6-4 2048 BITS
↳ ROW, COL, BYTES
AES (1 SBOX) 8-8 $2^8 \cdot 2^3 = 2^{11}$ BITS

S BOX DILEMMA
↳ LUTs
↳ COMPUTE ON FLY

DES PLUS SLIDES

DESX:

$$\underset{64}{K_3} \oplus E_{\underset{56}{K_2}}(\underset{64}{K_1} \oplus \underset{64}{m}) = 184$$

↑ TEXT ↑ KEY ↑ TEXT

AES: FINALLY ~~1997~~ 1997 → AES GETS MADE KINDA (NIST CALLS FOR DESIGN)

GF(2^K) → 2001 → FIPS (FEDERAL INFO PROCESSING STANDARD)
↳ AUTHENTICATED ENCRYPTION
↳ AES-GCM
↳ GALOIS COUNTER MODE
↳ GF(2^{128})
↳ RIJNDAEL BECOMES AES ← 8-BIT S-BOXES
↳ RUNS ON GF(2^8)

↳ CRYPTOCURRENCIES OFTEN RUN ON GF(2^{256})
↳ REALLY DON'T HAVE TO CARE

FIELDS:
GROUP ← 1 INVERTIBLE OP
↓ MAYBE
RING ← 2 INVERTIBLE OPS (+ & *)
↓
FIELD ← EVERYTHING WORKS

↳ F DOMAIN, +, *, 0, 1
↳ + * FINITE
↳ INVERTIBLE INFINITES
Q - RATIONAL
ℝ
ℂ - COMPLEX

FINITE FIELDS
~~NON-MOD~~ NON-MOD IN GF BIN. → NON-BIN. → GF(2^n) GF(p^n)
MODULAR MOD p → p - p ODD PRIME

GF.pdf SLIDES

★ SAYING THAT A POLYNOMIAL IS IRREDUCIBLE DEPENDS ON FIELD

IN $\mathbb{Z}_2$:

$x^2+1 = (x+1)^2$

IN $\mathbb{Z}_3$:

$f(x) = x^2+1$

x	f(x)
0	1
1	2
2	2

IF $f(x)$ IS IRREDUCIBLE THEN

$f(x) = (x-c)(x)$

PLUGGING ANY x IN THE DOMAIN IN RESULTS IN NON-ZERO VAL, SO NOT IRREDUCIBLE

AES: $x^8+x^4+x^3+x+1$ IRREDUCIBLE IN $\mathbb{Z}_2$

TEST GRADES WERE WONKY
↳ PEOPLE KEEP BITCHING
↳ SERIOUSLY, JUST LEARN FROM THE EXPERIENCE

NEXT HW IS OUT
↳ DUE 17 OCT.

PROVING IRREDUCIBILITY:
$f(x)$ IS IRREDUCIBLE IN $\mathbb{Z}_p$ IFF IT CANNOT BE FACTORED TO
$f(x) = g(x)h(x)$
$\deg(g), \deg(h) < \deg(f)$

SQUARE/MULT FOR x^y
① SEE INT y, BREAK BY BITS
EX: $x^{11} = ((x^2)^2 x^2)x$
BREAK INTO ORDERS OF 1 R 2
$11_{10} = 1011_2$

THEOREM:
LET p BE PRIME. THERE IS A UNIQUE FINITE FIELD OF ORDER p^n FOR EVERY $n \in \mathbb{Z}^+$. THIS FIELD IS USUALLY DENOTED $GF(p^n)$

$\mathbb{Z}_p[x]$
$p(x)$ IS IRREDUCIBLE } REST IN SLIDES

SMALL FIELDS

2	T/F, BITS
3	MOD 3
★ 4	$\{0, 1, \omega, \omega^2\} \cong \{0, 1, x, x+1\}$

WHAT CAN ω^2 BE?
$\omega^2 = \omega \Rightarrow \omega = 1$ ✗
SMALLEST NON-MODULAR FIELD

5	MOD 5
7	MOD 7
8	BINARY OCTAL GF
9	$GF(3^2)$

$x^3 + x + 1$ IS (BINARY) IRREDUCIBLE — 2^3 PRIME POWER

$f(x) = x^3 + x + 1$ HAS NO LINEAR FACTOR

$f(0) = 1$
$f(1) = 1$
NON-VANISHING POLYNOMIAL HAS NO LINEAR FACTORS
∴ IRREDUCIBLE

CAN BE REPRESENTED BY

$GF(2^8)$ CAN BE REP. BY $x^8+x^4+x^3+x+1$

NEEDS NO CUBIC, QUADRATIC, OR 4 FACTORS

Computing in GF(2^3) on x^3+x+1

$+ \rightsquigarrow$ bitwise XOR (mod 2)

$* \rightsquigarrow a_2x^2 + a_1x + a_0 \longleftrightarrow$ 3 bits

↳ Ex: $101 * 011$

$(x^2+1)(x+1) \bmod x^3+x+1$

$x^3+x^2+x+1 = x^2 = 100$

↳ Ex: $101 * 101$ — squaring in GF is term-by-term

$(x^2+1)(x^2+1) = (x^2+1)^2 = x^4+1$

added 0

$= x(x^3+x+1) + x^4+1$

$= x^4+x^2+x+x^4+1$

$= x^2+x+1 = 111$

$GF(9) = GF(3^2)$

$f(x) = x^2+1$ ← irreducible on $\mathbb{Z}_3$

$F = \{x+ya : +, *\}$, $a^2 = 2 \equiv a^2+1 = 0$ b/c mod 3

Ex: $(2+a)+(2+2a) = 1$

$(2+a)*(2+2a) = 2$

$f(0) = 1$
$f(1) = 2$ } no linear ∴ irreducible
$f(2) = 2$

F - vector space of dim. r over F_0 (prime field)

$\exists g \; \forall s \in F \quad s = g^i, \; 1 \le i \le q-1$

$g^i \cdot g^j = g^{i+j}$

$g = 1+a$ primitive in F

HW:

↳ 2: deg 4 over $\mathbb{Z}_2$

↳ ① No linear factors

② Divisible by x^2+x+1

↳ 4: For linear factors, test $x = 0, 1, 2, 3, 4$ (over $\mathbb{Z}_5$)

↳ Monic: poly where highest deg. poly is 1

↳ 5: $x^{12} \Rightarrow 12_{10} = 1100_2$

AES:

↳ NIST opened AES comp. in Jan 1997

↳ 15 candidates in Aug 1998

↳ 5 finalists in Aug 1999

↳ Mars

↳ RC6

↳ Rijndael

↳ Serpent

↳ Twofish

↳ Oct 2000, Rijndael was chosen

↳ Formally approved by federal standard in Nov 2001

128, 192, 256

K	# of rounds
128	10
192	12
256	14

AES:

↳ BYTE SUBSTITUTION

BYTES
ELEMENTS OF $GF(2^8)$

↳ SHIFT ROWS
↳ MIX COLS
↳ KEY ADDITION

MORE ABOUT BLOCK CIPHERS (CH 5)

↳ MODES OF OPERATION

ELECTRONIC CODE BOOK (ECB)

↳ BLOCK-BY-BLOCK ENCRYPTION
↳ SIMPLE
↳ "VULNERABLE" TO SUBSTITUTION ATTACKS

CIPHER BLOCK CHAIN (CBC)

↳ DIAGRAM IN BOOK

OUTPUT FEEDBACK MODE (OFB)

↳ SIMILAR TO CBC
↳ USED TO MAKE STREAM CIPHER

COUNTER MODE

↳ USES BLOCK CIPHER AS STREAM CIPHER

GALOIS COUNTER MODE

PUBLIC KEY CRYPTO

↳ MAILBOX CONCEPT
  ↳ ANYONE CAN PUT IN A LETTER, ONLY OWNER HAS KEY TO GET IT
↳ PUBLIC & PRIVATE KEY
  ↳ ENCRYPT W/ PUBLIC, DECRYPT W/ PRIVATE OR VICE VERSA
↳ SECURITY MECHANISMS
  ↳ KEY DISTRIBUTION: (DIFFIE-HELLMAN, RSA) W/OUT PRE-SHARED KEY
  ↳ NON-REPUDIATION & DIGITAL SIG.: (RSA, DSA, ECDSA) TO PROVIDE MESSAGE INTEGRITY
  ↳ IDENTIFICATION: CHALLENGE-RESPONSE PROTOCOLS W/ DIGITAL SIG.
  ↳ ENCRYPTION: (RSA, ELGAMAL) – COMPUTATIONALLY EXPENSIVE! (SLOWER THAN SYMMETRIC)

ET - EULER THEOREM

IF $\gcd(a,n)=1$ THEN

$a^{\varphi(n)} = 1 \bmod n$

FT - FERMAT THEOREM

p - PRIME, $1 \leq a < p$

SPECIAL CASE

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

$\Vert$

$a^{-1} = a^{p-2} \bmod p$

→ PROOF: $L = \prod_{r \in \mathbb{Z}_n^*} r = \prod_{r \in \mathbb{Z}_n^*} (ra) = a^{|\mathbb{Z}_n^*|} \prod_{r \in \mathbb{Z}_n^*} r$

LEMMA1: IF $\gcd(a,n)=1$ ↳ MULT BY a PERMUTES $\mathbb{Z}_n^*$

$\hookrightarrow a^{\varphi(n)} \cdot L$

LEMMA 2: L IS INVERTIBLE B/C IT IS THE PROD OF INVERTIBLES

EXAMPLE: $\mathbb{Z}_{18}^*$, $\varphi(18) = 6$

$\mathbb{Z}_{18}^*$: 1, 5, 7, 11, 13, 17

$L = 1 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \bmod 18$

$\downarrow *a \quad a = 5$

5, 7, 17, 1, 11, 13

} PERMUTATION = RESHUFFLE

RSA

RIVEST - SHAMIR - ALDEMAN

$n = pq$, p,q PRIMES, KEYS $ed = 1 \bmod \varphi(n)$

$\varphi(n) = (p-1)(q-1)$

$y = e_{K_{PUB}}(x) \equiv x^e \bmod n$

$x = d_{K_{PR}}(y) \equiv y^d \bmod n$

SPEEDING UP RSA

↳ SQUARE/MULTIPLY & OTHER FAST EXP

↳ PICK SHORT e, e=3

FOR RSA:

$\varphi(n)$ IS EVEN

↳ pq ARE ODD PRIMES

$\varphi(n) = (p-1)(q-1)$

e MUST BE ODD

↳ IF e IS EVEN THEN IT WOULD HAVE GCD W/ $\varphi(n)$ & INV WOULD NOT EXIST

CHINESE REMAINDER THEOREM - CRT

① $n = s \cdot t$, $\gcd(s,t) = 1$

$\mathbb{Z}_n = \{0, 1, 2, \ldots, 5, \ldots, n-1\}$

CRT: $\mathbb{Z}_n \xleftrightarrow[\text{ONTO}]{1\text{-}1} \mathbb{Z}_s \times \mathbb{Z}_t$

ISOMORPHIC

$x \xrightarrow{\text{EASY}} \begin{cases} x \bmod s \\ x \bmod t \end{cases}$

STD $\xleftarrow{\text{CRT}}$ (a, b)

Ex: $35 = 5 \cdot 7$ $\quad s=5,\ t=7$

$19 \rightsquigarrow (4, 5)$

$22 \rightsquigarrow (2, 1)$

$\mathbb{Z}_n$/STD $\qquad$ CRT

$\bmod s$ / $\bmod t$ — get $\begin{cases} s^{-1} \bmod t \\ t^{-1} \bmod s \end{cases}$

$(0,1) \cong s(s^{-1} \bmod t)$

$(1,0) \cong t(t^{-1} \bmod s)$ $\Rightarrow (a,b) = a(1,0) + b(0,1) = \underbrace{at(t^{-1} \bmod s) + bs(s^{-1} \bmod t)}_{\text{MODULO } n}$

$1 \bmod s$; 0 modulo t

$n = 35,\ s = 5,\ t = 7$

$5^{-1} \bmod 7 = 3$

$7^{-1} \bmod 5 = 3$

$(0,1) = 15$

$(1,0) = 21$

$(3,4) = (3 \cdot 21 + 4 \cdot 15) \bmod 35$

$= 18$

SQ & MULTIPLY

Ex) $19^{22} \bmod 35$ — VIA CRT

$19 \rightarrow (4, 5)$

$(4,5)^{22} = (4^{22}, 5^{22})$

$4 \bmod 5 = -1$

$5 \bmod 7 = -2$

$\bmod 5$ $\qquad$ $\bmod 7$

-1 TO EVEN POWER $= (1, ((-2)^2)^{11})$

$= (1, 2)$

STD $\Rightarrow (1 \cdot 21 + 2 \cdot 15) \bmod 35$

$= 51 \bmod 35 = 16$

GOES AWAY B/C MULT OF $\varphi(7)$ EULER

$5^{22} = 5^{3 \cdot 6 + 4} = (-2)^4$

$= 2^4$

$= 2$

MULTIMODULOUS CRT

$m_1, \ldots, m_k \quad i \neq j \rightarrow \gcd(m_i, m_j) = 1$

$M = \prod m_i, \quad \text{mod } M \leftarrow$ BIG ARITHMETIC

$\text{mod } m_i \leftarrow$ SMALL ARITH

$m_1 = 3$
$m_2 = 5$
$m_3 = 7$

$M = 105$

i	1	2	3
m_i	3	5	7
M_i	35	21	15
M_i^{-1}	2	1	1

$35^{-1} \bmod 3$
$= 2 \bmod 3$
$2^{-1} \bmod 3 = 2$

BASIS VECTORS
$(000 \ldots 1000)$

$M_i = \frac{M}{m_i} \longleftrightarrow M_i (M_i^{-1} \bmod m_i)$

$(100) \rightsquigarrow 70$
$(010) \rightsquigarrow 21$
$(001) \rightsquigarrow 15$
$(a,b,c) \rightsquigarrow (70a + 21b + 15c) \bmod 105$

$33 + 12 = 45$
$(0,3,5) + (0,2,5) = (0,0,3)$

IF $k=2$
↳ $S = m_1$
↳ $t = m_2$
↳ $M_1 = t$
↳ $M_2 = S$
} LAST PAGE

TASK
COMPUTE ALL $\sqrt{1}$S IN $\mathbb{Z}_{105}$
(SOLVING $x^2 = 1 \bmod 105$)

THE ROOTS ARE:
$(\pm 1, \pm 1, \pm 1)$

```
- - -
- - +
- + -
(-1,1,1) - + +
+ - -
(1,-1,1) + - + ⇝ 70 - 21 + 15 = 64
+ + -
+ + +
```

$64^2 \equiv 4096 \bmod 105$
$= 1$

PRIME NUMBERS

$n = 110792355103$
$= p \cdot q$?

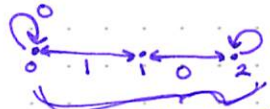
IS THERE A $p \leq 10^7$ DIVIDING n?

NAIVE SEARCH NEEDS $\sqrt{n}$ DIVISIONS
↳ NOT POLYNOMIAL, BUT EXPONENTIAL IN LOG(n)

MERSENNE PRIMES
$M_p = 2^p - 1$

GIMPS
GREAT INTERNET MERSENNE PRIME SEARCH

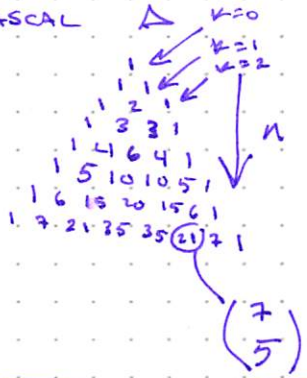
FIND IF BINARY VAL IS DIVISIBLE BY 3:



LEARN MILLER-RABIN?

AKS
↳ AGARWAL, KAYAL, SAXENA

PASCAL Δ



$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

THM: n DIVIDES ALL $\binom{n}{k}$ IFF n IS PRIME

DONUM ZEILBERGER BOOK
↳ $a = b$

AKS ALGORITHM
↳ IN POLY TIME: $O((\log^{12} n)\,\text{poly}(\log\log n))$ - time

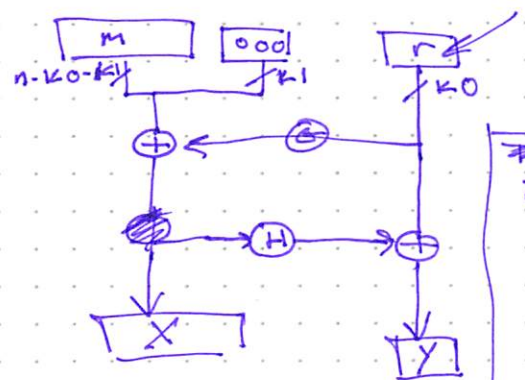
FERMAT THM:
IF a IS REL. PRIME TO p
↳ $a^{p-1} \equiv 1 \bmod p$

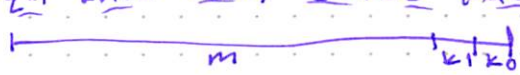
BASIC CONGRUENCE (AKS)
- a & n ARE REL PRIME
- n IS PRIME IFF $(x-a)^n \equiv (x^n - a) \bmod n$

$$(x-a)^n \bmod n = \sum_{k=0}^{n} \underbrace{\binom{n}{k} \bmod n}\, x^k (-a)^{n-k}$$

RECOMMENDATION FOR RSA
↳ $n \approx 2^{2048}$ OR MORE
↳ pq SIMILAR IN SIZE
↳ e CAN BE SMALL, d BETTER FULL SIZE
↳ ENCLOSE IN SHELL LIKE OAEP
↳ OPTIMAL ASYM ENC. PADDING
↳ DON'T USE "NORMAL" CRT
↳ VULNERABLE TO SIDE-CHANNEL & FAULT INJECTION
↳ AVOID PRIMES p, q SUCH THAT $p-1, q-1$ HAVE MANY SMALL FACTORS

OAEP & RSA





k0 = k1 = 128

REVERSIBLE

FACTORING $n = p \cdot q$ OFTEN CAN BE DONE BY SOLVING
$x^2 = 1 \bmod n$

$(x-1)(x+1) = 0 \bmod n$
$p \quad q$
$q \quad p$
pq
pq

TRYING $35 = 5 \cdot 7$
$x^2 = 1$? $x = 6$
$5 \cdot 7 = 0 \bmod 35$

POLLARD RHO FACTORING ALG. (n, x_1)

X IS FINITE
$|X| = n$

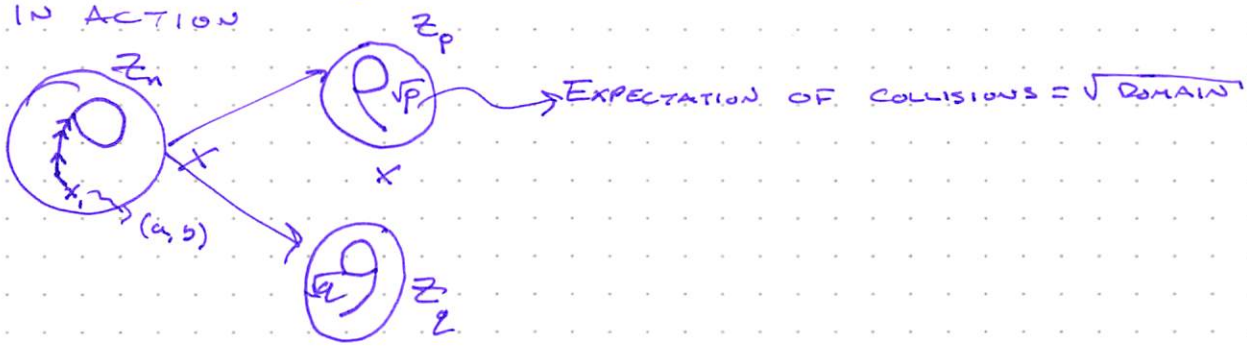
$f: X \to X$

EVENTUALLY CYCLIC

$n = p \cdot q$, $p \leq q$, $p = O(n^{1/2})$

RESULT: VERY LIKELY FACTORS n IN TIME $O(n^{1/4})$

- FACTORS IN $O(n^{1/4})$ TIME
- MEMORYLESS CYCLE DETECTION
- CRT IN ACTION
  - ↳ ?



DISCRETE LOGARITHM

$x \xrightarrow{\exp,\ y} x^y \bmod n \xrightarrow{\log} y$

DL DISCRETE LOG
FIX x, n
TASK: FIND y

DIFFIE-HELLMAN

DHKE SET UP
1) CHOOSE LARGE PRIME
2) CHOOSE AN INTEGER $\alpha \in \{2, 3, \ldots, p-2\}$
3) PUBLISH p & α

~~BIRTHDAY PARADOX~~ B-DAY PARADOX
CH 9: ECC

HASH & SIGN
CH 10: SIGNATURES
CH 11: HASHING
CH 12: KEY MGMT

① RSA w/ SWAPPED KEYS
② DSA - DIGITAL SIG. ALG.
↳ MODULAR BASED
③ ECDSA
↳ BITCOIN

RSA $n = p \cdot q$

$(x^e)^d = x = (x^d)^e \bmod n$

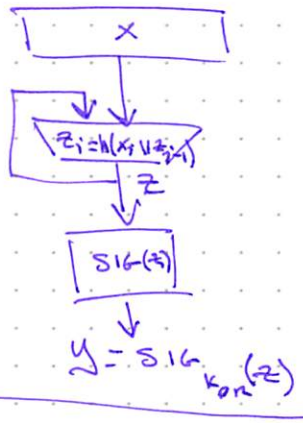
e: ENC. (KDEC) — d: SIGN (VERIFY)

GEN SIG: $S = SIG_{K_{priv}}(x) = x^d \bmod n$

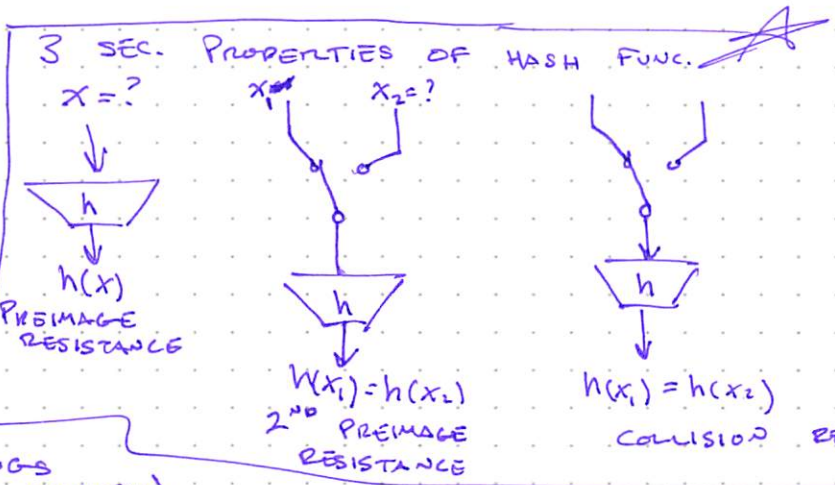
VERIFY SIG: $x' = VER_{K_{pub}}(S) = S^e \bmod n$
IF $x = x'$, SIGNATURE IS VALID

HASHING:
MD5 (RIVEST) 128 BITS
SHA-0 — X
SHA-1 — STRONG → 160 BITS
SHA-2 ~ NEW STD
SHA-3 → COMING STRONG → 256, 384, 512
2014 ↓

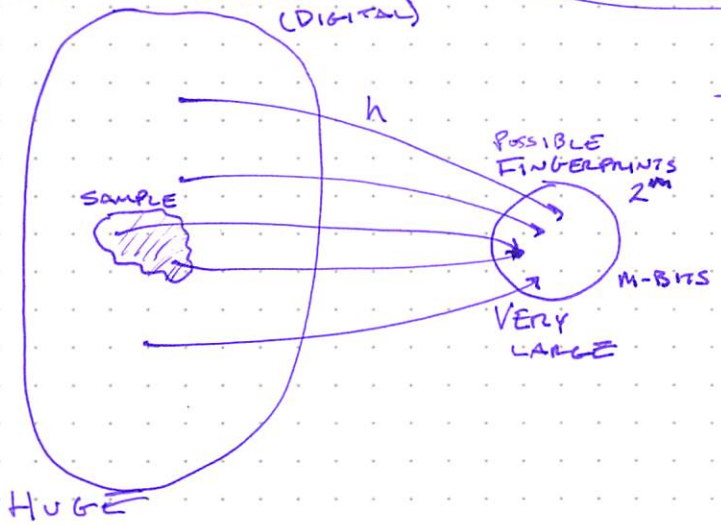
DIGITAL SIGNATURE W/ A HASH FUNC.



3 SEC. PROPERTIES OF HASH FUNC.



X = ALL THINGS (DIGITAL)



THM: SAMPLING $1.17\sqrt{2^m}$ ITEMS FROM X PRODUCES A COLLISION $h(x_1) = h(x_2)$ W/ LIKELIHOOD $\geq 1/2$

HASH FUNCTION: ALGORITHMS

HASH ALG:

- SPECIAL ALGS
- BASED ON BLOCK CIPHERS

BIRTHDAY ATTACK

$$1 - \varepsilon = \left(\frac{m-1}{m}\right)\left(\frac{m-2}{m}\right)\cdots\left(\frac{m-q+1}{m}\right) \qquad m = \text{SIZE OF HASH SPACE}$$

$$= \prod_{i=1}^{q-1}\left(1 - \frac{i}{m}\right) \doteq \prod_{i=1}^{q-1} e^{\frac{i}{m}}$$

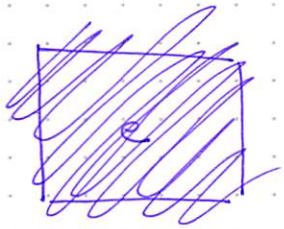
$$= e^{\sum_{i=1}^{q-1} -\frac{i}{m}} = e^{\frac{-q(q-1)}{2m}}$$

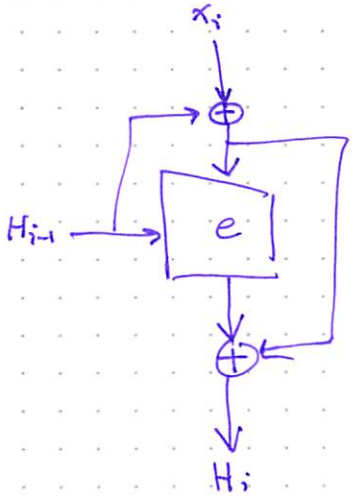
HENCE: $\frac{-q(q-1)}{2m} \doteq \ln(1-\varepsilon)$

(SLIDES 19-21)

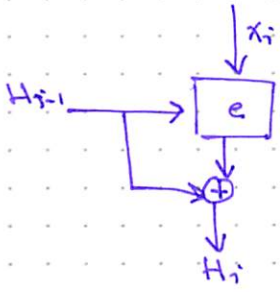
11.3.2

$e(H_{i-1}, x_i \oplus H_{i-1}) \oplus (x_i \oplus H_{i-1})$

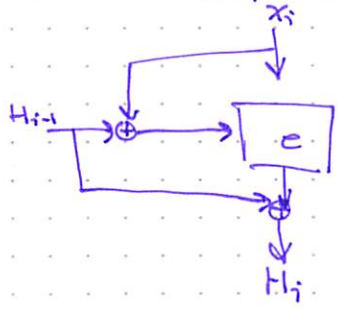




11.3.5 $e(x_i, H_{i-1}) \oplus H_{i-1}$



11.3.8 $e(x_i, x_i \oplus H_{i-1}) \oplus H_{i-1}$



11.3.11 $e(x_i \oplus H_{i-1}, x_i) \oplus H_{i-1}$