Biomedical Security

Erwin M. Bakker

SC MEDIA

"Brute force and dictionary attacks up 400 percent in 2017"

Feb 28, 2018 News by Rene Millman

Researchers Used Sonar Signal From a Smartphone Speaker To Steal Unlock Passwords (vice.com)

https://www.schneier.com/

HEALTHCARE

Top 10 Biggest Healthcare Data Breaches of All Time

by Nate Lord on Monday June 25, 2018

https://digitalguardian.com

REPORT

Botched CIA Communications System Helped Blow Cover of Chinese Agents

The number of informants executed in the debacle is higher than initially thought.

https://foreignpolicy.com/2018/08/15/

Your Router's Security Stinks: Here's How to Fix It

by PAUL WAGENSEIL May 29, 2018, 5:52 AM

https://www.tomsguide.com

Overview

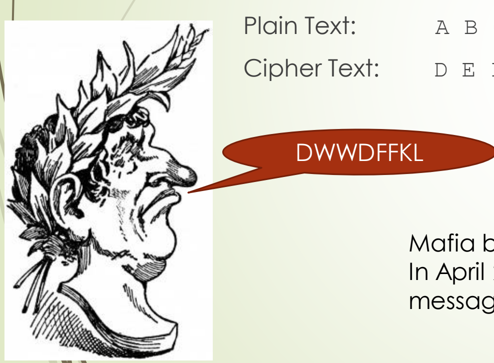
- Cryptography: Classical Algorithms,
- Cryptography: Public Key Algorithms
- Cryptography: Protocols
- Pretty Good Privacy (PGP) / B. Schneier Cryptography Workshop
- Biomedical Security and Applications
- Student Presentations
- Student Presentations

Grading:
Class participation, assignments (3 out of 4)
(workshop + presentation + technical survey)/3

Cryptography: Sharing Secrets

- CAESAR a substitution cipher

Secret Key: 3
Plain Text: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher Text: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C



E_3(HELP) = KHOS
D_3(KHOS) = HELP

$D_3 = E_{26\text{-}k}$

Mafia boss Bernardo Provenzano's cipher: 'A' -> 4, 'B' -> 5, etc.
In April 2006, Provenzano was captured in Sicily partly because messages encrypted using his cipher, were broken.

https://www.theregister.co.uk/2006/04/19/mafia_don_clueless_crypto/

Cryptography: Sharing Secrets

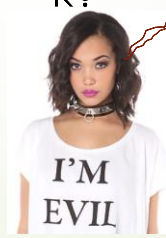
Alice

$C = E_K$ ('HELLO BOB')

Secret key K

Crypto-text C

K?



Eve

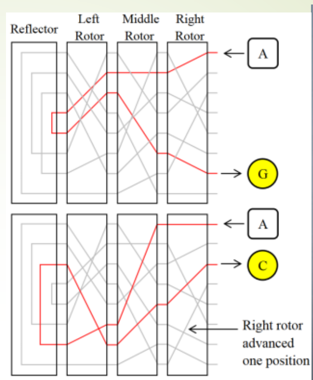
Bob

D_K (C) = 'HELLO BOB'

Secret key K

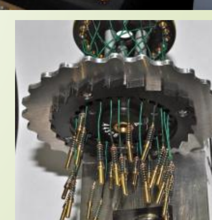
Crypto-Analyst Eve
- Crypto-text only
- Known Plaintext
- Chosen Plaintext

Enigma



Encryption as a product of permutations:

- P the plug-board transformation
- U the reflector
- L, M, and R the three rotors
- Then encryption is $E = PRMLUL^{-1}M^{-1}R^{-1}P^{-1}$
- After each key press the rotors turn i positions changing the transformation: R becomes C^iRC^{-i}, where C is the cyclic permutation (A->B, B-> C, etc. …)
- the military Enigma has 158,962,555,217,826,360,000 settings **(?)**



https://en.wikipedia.org/wiki/Enigma_machine

http://enigmamuseum.com/replica/

ONE-TIME PAD

- A crypto system with perfect secrecy

Plaintext:	01000110101110100110
Key:	11010100001100010010
Crypto-text:	10010010100010110100

Uses XOR for both encryption and decryption.

Classical Symmetric or Two-way Crypto Systems

- A shared secret key K used for both encryption as well as decryption.

Secret Key	K
Plaintext	P
Crypto-text	C

$C = E_K(P)$

$P = E^{-1}_K(C)=D_K(C)$

Classical Symmetric Crypto System: Data Encryption Standard (DES)

- March 17, 1975 published by the National Bureau of Standards (NBS)
- NSA reduced key-size from the original 128-bit to 56-bit
- At the time NSA studied it and said it was secure to use as a standard SKCS.
- Next government standard was classified: Skipjack

- Block cipher encrypting data in 64-bit blocks
- Key length 56-bits
- 16 rounds: in each round a substitution followed by a permutation

Feistel Networks

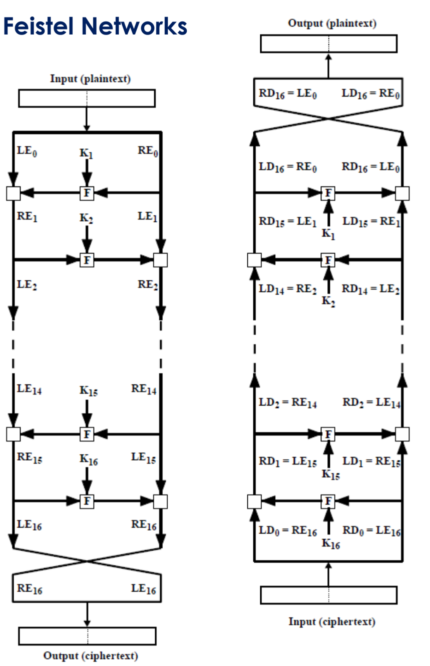
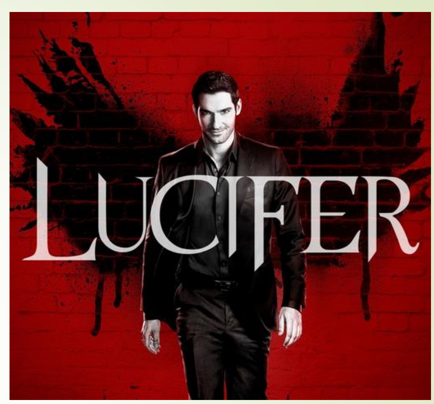


Figure 3.6 Feistel Encryption and Decryption



IBM's Cipher LUCIFER designed by H. Feistel and D. Coppersmith in 1973 used Feistel Networks for encryption and decryption.

LUCIFER is one of the first commercial block ciphers on which DES is based.

Encryption of the Text

Processing of the Key

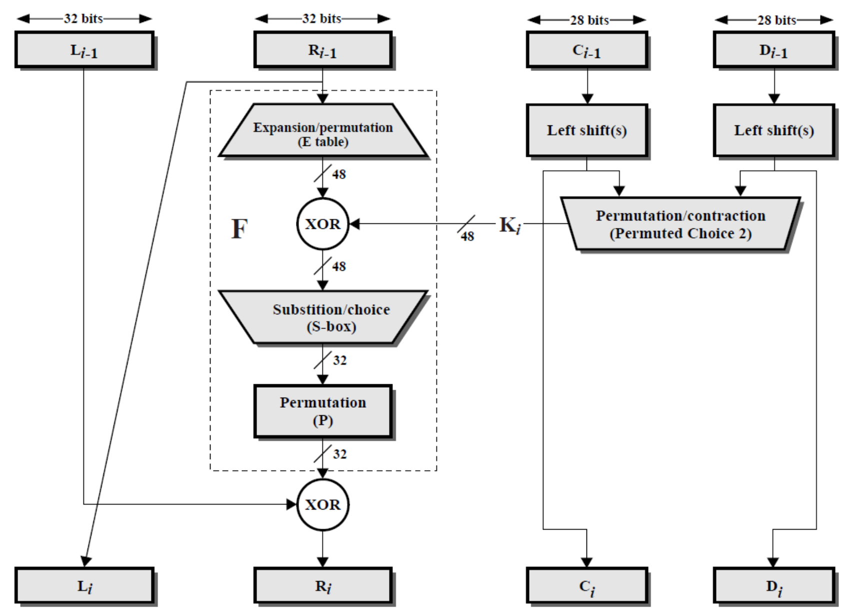
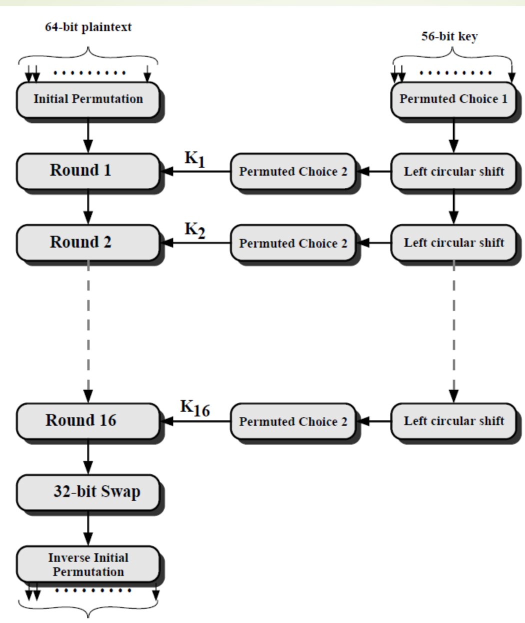


Figure 3.8 Single Round of DES Algorithm



Encryption in DES

13

Classical Symmetric Crypto System: International Data Encryption Algorithm (IDEA)

IDEA is a Block Cipher designed by X. Lai and J. Massey in 1990. Revised in 1991 to withstand differential cryptanalysis.

- **Block Length**

  64-bit Data Blocks Is considered safe against statistical attacks. Cipher Feedback Mode enhances cryptographic strength.
- **128-bit Key**

  Safe against brute-force attacks.
- **Good Confusion**

  By using three operations: XOR, Addition mod 2^{16}, Multiplication mod $2^{16}+1$ (compare with DES: XOR, small S-Boxes)
- **Good Diffusion**

  Every plaintext bit and every key-bit influences every ciphertext bit.

14

Symmetric Cryptosystem: BLOWFISH

Blowfish is a symmetric block cipher

designed by Bruce Schneier in 1993.

- **Block Length**

  64-bit data blocks encrypted in 64-bit ciphertext Blocks.
- **Key Length**

  32- 448 bits (1 to 14 32-bit key-blocks).
- **Variable Security**

  Key generates 18 (32-bit) subkeys, and 4 (8x32 bit) S-boxes. The algorithm itself is used for this.
- **Fast, simple, and compact**

  On a 32-bit processor: 18 clock cycles per encrypted byte. Uses less than 5K of memory (was at the time too big for smart-cards).

15

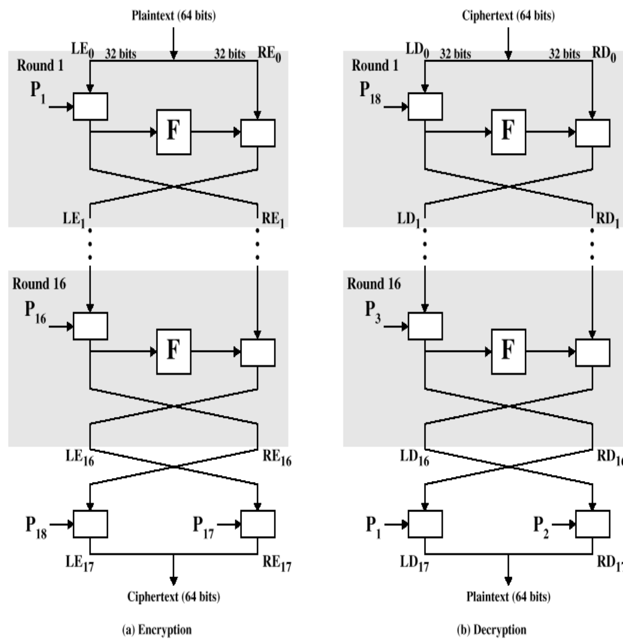


Figure 4.9 Blowfish Encryption and Decryption

16

Rivest Cipher 5 (RC5)

RC5 is a block-cipher by R. Rivest in 1994.

- **Efficient Hard and Software Implementations**

  Simple structure, simple operations, low memory requirements, fast and simple implementations.

- **Variable Word Length:**

  w = 16, 32,or 64 Length of the plaintext blocks is 2w

- **Variable Key-Length**

  b = 0,...,255 bytes

- **Variable Security**

  Depending on the parameters, number of rounds: r = 0,…,255

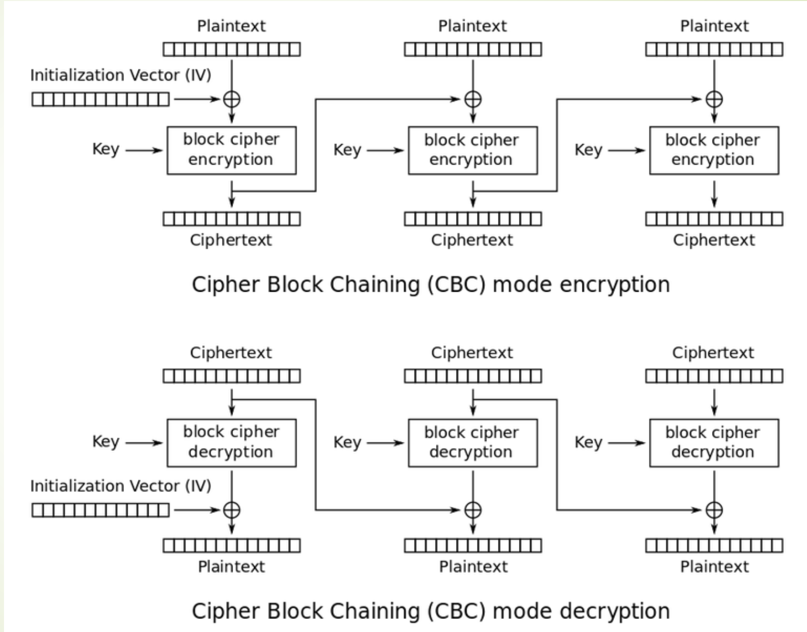
- **Data-Dependent Rotations**

  Circular Bit Shifts. RC5-w/r/b = RC5-32/12/16 considered to have "Nominal" Security. Incorporated in the products BSAFE, JSAFE, and S/MAIL of RSA Data Security, Inc.

17

Rivest Cipher 5 (RC5) Modes

- Block Cipher Mode
- Cipher Block Chaining Mode
- RC5-CBC-Pad
- RC5-CTS Ciphertext Stealing Mode: CBC style.



18

CAST-128

A symmetric encryption cipher by

C. Adams and S. Tavares in 1997.

- Uses four primitive operations

  addition and substraction mod 2^{32}, XOR, left circular rotations.
- Uses fixed non-linear S-boxes, also for sub-key generation.
- A function F is used with good confusion, diffusion, and avalanche properties.
  - its strength is based on the S-boxes. F differs per round.
  - increase of strength of CAST-128 using more rounds is not (yet) demonstrated.
- 64-bits data blocks
- 40- 128-bits key

CAST-128 is used in PGP.

19

Rivest Cipher 2 (RC2)

A symmetric encryption cipher by

R. Rivest in 1997.

- Designed for 16-bit microprocessors
- Uses 6 primitive operations

  addition and subtraction mod 2^{32}, XOR, COMPL, AND, and Left Circular Rotation.
- No Feistel Structure.
- 18 rounds: 16 mixing rounds, and 2 mashing rounds.
- 64-bits data blocks
- 8 - 1024-bits key

RC2 is used in S/MIME with 40-, 64-, and 128-bits keys.

RC2 is vulnerable to a related-key attack using 2^{34} chosen plaintexts (Kelsey et al., 1997).

20

Characteristics of Advanced Symmetric Block Ciphers

- **Variable Key Length** Blowfish, RC5, CAST-128, and RC2
- **Mixed Operators**
- **Data-Dependent Rotation** An alternative to S-boxes. No dependence on sub-keys. RC5.
- **Key-Dependent Rotation** CAST-128
- **Key-Dependent S-Boxes** Blowfish
- **Lengthy Key Schedule Algorithm** Against brute-force attacks. Blowfish
- **Variable F** to complicate cryptanalysis. CAST-128

21

Advanced Symmetric Block Ciphers

- **Variable Plaintext/Ciphertext Block Length**

  For convenience and cryptographic strength (longer blocks is better) RC5
- **Variable Number of Rounds**

  More rounds increase cryptographic strength. Trade-off between execution time and security. RC5
- **Operation on Both Data Halves in Each Round**

  AES, IDEA, Blowfish, and RC5

Advanced Encryption Standard (AES)

- Block-size: 128
- Key-sizes: 128, 192, 256
- NIST Specification 2001
- Origin: a subset of 3 out of the Rijndael Cipher by V. Rijmen and J. Daemen (NIST paper 2003)
- Substitution-permutation network
- From the cipher key the keys per round are derived.
- Each round
  - has a non-linear substitution step implemented using a lookup table
  - Followed by transposition using cyclic shifts
  - And a mixing step on the columns of the internal state matrix.
  - The round ends with an add key operation.

A Short Introduction to Number Theory

- Primes
- Factorization
- Euclid's Algorithm
- Modular Arithmetic and Groups
- Fast Exponentiation
- Discrete Logarithms
- Euler Phi

24

Number Theory

Definition (Divisors):

$b \neq 0$ divides a, if a = mb for some m (where a, b, and m are integers)

Notation: b | a

Example: divisors of 24 are

1, 2, 3, 4, 6, 8, 12, and 24

The following relations hold:

- if a | 1, then a = ±1
- if a | b and b | a, then a = ±b
- any $b \neq 0$ divides 0
- if b | g and b | h, then b | (mg+nh) for arbitrary integers m and n

25

Number Theory

Definition (Prime Numbers):

An integer p>1 is a prime number if its only divisors are ±1 and ±p.

Theorem: Any positive integer a>1 can be factored in a unique way as:

$$a = p_1^{a1}.p_2^{a2}\ldots p_t^{at},$$
where $p_1 > p_2 > \ldots > p_t$ are prime,
and $a_i > 0$

$$\text{or } a = \prod_{i=1\ldots t} p_i^{a_i}, \text{ where } p_1 > p_2 > \ldots > p_t \text{ are prime and each } a_i \geq 0$$

Example: 91 = 7 x 13,
11011 = 7 x 11^2 x 13

26

Number Theory

Definition1 (GCD):

The positive integer c is said to be the greatest common divisor of a and b if:

1) c | a and c | b
2) if d | a and d | b, then d | c

Notation: c = gcd(a,b)

Definition2 (GCD):

gcd(a,b) = max[k, such that k | a and k | b]

Example: 192 = 2^2 x 3^1 x 4^2
18 = 2^1 x 3^2
gcd(18,192) = 2^1 x 3^1 x 4^0 = 6

27

Number Theory

Definition1 (Relative Prime):
The integers a and b are said to be relatively prime if gcd(a,b) = 1.

Example:
192 and 18 are not relatively prime:

$192 = 2^2 \times 3^1 \times 4^2$

$18 = 2^1 \times 3^2$

$\gcd(18,192) = 2^1 \times 3^1 \times 4^0 = 6$

74 and 75 are relatively prime:

$74 = 2 \times 37$

$75 = 3 \times 5^2$

$\gcd(74,75) = 1$

28

Number Theory: Modular Arithmetic

Given any positive integer n and any integer a we can write:

$a = qn + r$, where $0 \leq r < n$, $q = \lfloor a/n \rfloor$

r is called the **residue** (mod n)

Definition: If a is an integer and n is a positive integer we define *a mod n* to be the remainder when a is divided by n.

Thus, $a = \lfloor a/n \rfloor \times n + (a \bmod n)$

Definition: Two integers are said to be congruent modulo n if

$(a \bmod n) = (b \bmod n)$

Notation: $a \equiv b \bmod n$

29

Number Theory: Modular Arithmetic

Examples: $73 \equiv 4 \bmod 23$ as
$73 = 3 \times 23 + 4$, hence
$4 = 73 \bmod 23$, and clearly
$4 = 4 \bmod 23$

$21 \equiv -9 \bmod 10$ as
$1 = 21 \bmod 10$ and
$1 = -9 \bmod 10$

Properties (Check):

- $a \equiv b \bmod n$ if $n \mid (a-b)$
- $(a \bmod n) = (b \bmod n)$ implies $a \equiv b \bmod n$
- $a \equiv b \bmod n$ implies $b \equiv a \bmod n$
- $a \equiv b \bmod n$ and $b \equiv c \bmod n$ implies $a \equiv c \bmod n$

30

Number Theory: Modular Arithmetic

The mod n operator maps all integers into the set of integers $Z_n = \{0,1,\ldots,(n-1)\}$, the set of all residues modulo n.

The following properties hold for modular arithmetic within Z_n:

- $(w + x) \bmod n = (x + w) \bmod n$
- $((w+x)+y) \bmod n = (w+(x+y)) \bmod n$
- $(0+w) \bmod n = w \bmod n$
- $\forall w \in Z_n \exists z \in Z_n$ such that $w + z \equiv 0 \bmod n$

- $(w \times x) \bmod n = (x \times w) \bmod n$
- $((w \times x) \times y) \bmod n = (w \times (x \times y)) \bmod n$
- $(1 \times w) \bmod n = w \bmod n$
- $(w \times (x+y)) \bmod n = ((w \times x)+(w \times y)) \bmod n$

31

Number Theory: Modular Arithmetic

Z_8:	0	1	2	3	4	5	6	7
×6:	0	6	12	18	24	30	36	42
mod 8:	0	6	4	2	0	6	4	2

Z_8:	0	1	2	3	4	5	6	7
×5:	0	5	10	15	20	25	30	35
mod 8:	0	5	2	7	4	1	6	3

Note: gcd(6,8) = 2, and gcd(5,8) = 1

Notation: $Z_p^* = \{1,2,\ldots,(p-1)\}$

Theorem: Let p prime, then for each $w \in Z_p^*$ there exists a z such that $w \times z \equiv 1 \bmod p$, z is equal to the multiplicative inverse w^{-1} of w

32

Public-Key Cryptography Fast Exponentiation

Calculate $a^b \bmod n = 7^{560} \bmod 561$

a = 7, b = 560 = 1000110000, n = 561

		Exponent	result	
I	b_i	c	d	->7^{560}
9	1	1	7	7^1
8	0	2	49	7^2
7	0	4	157	7^4
6	0	8	526	7^8
5	1	17	160	7^{16+1}
4	1	35	241	7^{32+2+1}
3	0	70	298	7^{64+4+2}
2	0	140	166	$7^{128+8+4}$
1	0	280	67	$7^{256+16+8}$
0	0	560	1	$7^{512+32+16}$

```
c ← 0; d ← 1
for i ← k downto 0
    do c ← 2 × c
       d ← (d × d) mod n
       if  bi = 1
           then c ← c + 1
                d ← (d × a) mod n
return d
```

33

Number Theory: Euler Totient Function

Definition: The Euler's totient function $\Phi(n)$ of n is equal to the number of positive integers <n that are relative prime to n.

Examples:

8: {1,3,5,7} are relative prime to 8 and <8, thus $\Phi(8) = 4$

11: {1,2,3,4,5,6,7,8,9,10} are relative prime to 11 and <11, thus $\Phi(11) = 10$

Lemma: If p is prime, then $\Phi(p) = p - 1$.

Lemma: If n = pq, with p and q prime, then $\Phi(n) = (p-1)(q-1)$.

Proof: {p,2p,…,(q-1)p}, {q,2q,…,(p-1)q}, and 0 are not relatively prime. Thus $\Phi(n) = pq - (q-1) - (p-1) - 1 = (p-1)(q-1)$.

34

Number Theory: Euler's Totient Function

Fermat's Theorem (1640): For every prime p and any integer a, the following holds:

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

Euler's Theorem (~1740): For any positive integer n, and any integer a relative prime to n, the following holds:

$$a^{\Phi(n)} \equiv 1 \bmod n$$

Corollary: Let p,q be prime, and n = pq, m an integer such that gcd(m,n)=1, then

$$m^{(p-1)(q-1)} \equiv 1 \bmod n$$

Examples:

$\mathbf{2^6 = 64 = 63 + 1} \equiv 1 \bmod 7$

$4^{(5-1)(7-1)} = 4^{24} = (4^8)^3 \bmod 35 \equiv 16^3 \bmod 35 \equiv 4096 \bmod 35 \equiv 1 \bmod 35$

35

Number Theory: Testing for Primality

[Miller'75, Rabin'80]

Procedure Witness(a,n) n is to be tested for primality, a is some integer less than n.

if (not $a^{n-1} \equiv 1 \bmod n$) or
($\exists x$: $x^2 \equiv 1 \bmod n$ and $x \neq \pm 1$)
then return TRUE {n is no prime}
else return FALSE {n may be prime}

If n is no prime the probability that Witness returns FALSE is <0.5.
Thus, if Witness returns FALSE s times the probability that n is prime is at least $1 - 2^{-s}$.

36

Number Theory: Number of Primes

Definition: $\pi(n)$ is equal to the number of primes p that satisfy $2 \leq p \leq n$.

Theorem (The Prime Number Theorem, conjectured by Legendre, Gauss, Dirichlet, Chebyshev, and Riemann; proven by Hadamard and de la Vallee Poussin in 1896).

$$\pi(n) \sim n/\ln(n)$$

Thus there are about

$$10^{100}/\ln(10^{100}) - 10^{99}/\ln(10^{99}) =$$

$$0.039 \times 10^{99} \text{ 100-digit primes}$$

There are 4.5×10^{99} 100-digit odd numbers.

That is, about 1 of every 115 100-digit odd numbers is prime.

37

Number Theory: Euclid's Algorithm
Finding the Greatest Common Divisor

Theorem: For any integer a≥0, and any integer b>0: gcd(a,b) = gcd(b,a mod b)

Proof: Let d = gcd(a,b) => d | a and d | b => a = kb + a mod b for some integer k => (a mod b) = a -kb => d | (a mod b) (as d | a and d | kb). Thus d is a common divisor of b and (a mod b).

Conversely, if d = gcd(b, a mod b), then d | kb and thus also d | (kb + a mod b) => d | a. Thus d is also a common divisor of a and b.

qed

Example (Calculation of GCD):

- gcd(12,18) = gcd(18,6) = gcd(6,0) = 6
- gcd(10,11) = gcd(11,1) = gcd(1,0) = 1

38

Number Theory: Euclid's Extended Algorithm
Finding the Multiplicative Inverse

If gcd(d,n) = 1, then (d^{-1} mod n) exists.

I.e., dd^{-1} = 1 mod n.

Complexity: The multiplicative inverse can be found in O($\log^2 n$) time.

39

Number Theory: Discrete Logarithm

Definition: Let $Z_n^*=\{1,2,\ldots,(n-1)\}$, and g in Z_n^*. Then any integer x such that:

$$g^x = y \bmod n$$

is called a *discrete logarithm of y to base g.*

Example:

Z_7^*	1	2	3	4	5	6
	3^1	3^2	3^3	3^4	3^5	3^6
g=3	3	2	6	4	5	1

Z_7^*	1	2	3	4	5	6
$\log_3$	6	2	1	4	5	3

N.B. g=3 is a generator of Z_7^*

Definition: If for g in Z_p^* $\{g^1,\ldots,g^{(p-1)}\} = Z_p^*$ holds, then g is a *generator* of Z_p^*.

40

Number Theory: Complexity of PRIMES, Discrete Log, FACTORIZE, etc.

- Finding Primes (PRIMES is in P, AKS-Algorithm, August 2002)

After 1/115 tries success. Each try fastexp and some tests are executed => O(log n) time.

- Finding Safe Primes

It is unknown whether there exist infinitely many safe primes.

- Calculating the Discrete Logarithm

If the prime factors of (p-1) are small there exist efficient algorithms, otherwise roughly the same complexity as factorising.

- Factorising n (b-bits)

  Peter Shor(1994): $O(b^3)$ and O(b) space on a quantum computer.

  Kleinjung et al. (2010) used general number field sieve GNFS- approach,

  $O(e^{\sqrt[3]{\frac{64}{9}b(\log b)^2}}$ time, for the factorization of a 768-bit RSA modulus n.

- Calculating Euler's Phi Function of n

It is unknown if this can be done without factorising n.

- Finding the multiplicative inverse mod n

$O(\log^2 n)$