Biomedical Security

Erwin M. Bakker

Some Security News

- Blockchains are not safe for voting (slashdot.org) :

From: NYTimes

Expert Panel Calls for Sweeping Election Security Measures

By The Associated Press

Sept. 6, 2018

BOSTON — An expert panel of the National Academy of Sciences called for fundamental reforms to ensure the integrity of the U.S. election system, which is handicapped by antiquated technology and under stress from foreign destabilization efforts.

Biometric and App Logins Will Soon Be Pushed Across the Web

Google, Microsoft, and Mozilla are supporting WebAuthn, a login standard so users more easily access services without a password, and instead use fingerprint data, a hardware token or an app.

From Motherboard.vice.com

By Joseph Cox | Apr 10 2018, 12:00pm

ECDAA: Eliptic Curve Direct Anonymous Attestation for remote authentication of a trusted computer while preserving privacy of the user (Wikipedia)

Takeaway

1. Invalid curve attacks leak your secret key
2. Nonce reuse in ECDSA leaks your secret key
3. Elliptic Curve Cryptography parameter choice is a very complicated issue best left to experts (who will still take years to arrive at a satisfactory answer)
4. Don't roll your own crypto

From: paragonie.com

Worries arise about security of new WebAuthn protocol

Cryptography experts point out that new WebAuthn protocol recommends or requires the implementation of old and weak algorithms known to be vulnerable to attacks for years

By Catalin Cimpanu for Zero Day | September 9, 2018 -- 01:06 GMT (02:06 BST) | Topic: Security

In short: PKCS1v1.5 is bad. The exploits are almost old enough to legally drink alcohol in the United States. Don't use it!

From: paragonie.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

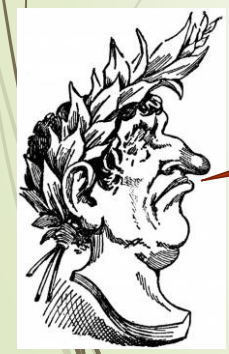
Cryptography: Sharing Secrets

- 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



DWWDFFKL

E_3(HELP) = KHOS

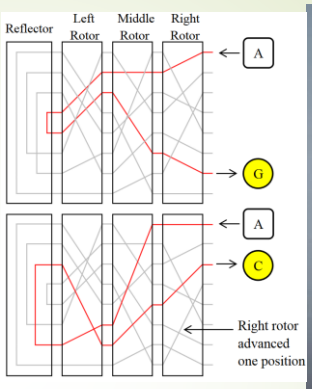
D_3(KHOS) = HELP

$D_3 = E_{26-k}$

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/

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.

Plaintext P

Crypto-text C

$C = E_K(P)$

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

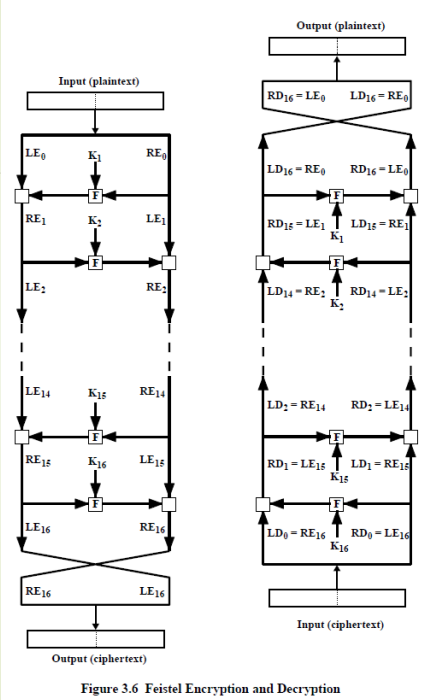
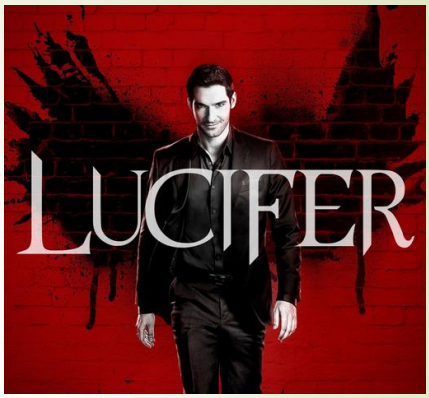


Figure 3.6 Feistel Encryption and Decryption



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.

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

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.

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

How?

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

Public Key Crypto Systems

Idea by Diffie and Hellman [1976]

- Encryption method made public.
- Decryption method kept secret.

Closely related to the idea of cryptographic one-way functions:

x —easy→ f(x)

f(x) —intractable→ x

But there exists a trapdoor that makes it easy to calculate x given f(x).

Note: No known cryptographic one-way functions. Only likely to be intractable!

Intractability and P = NP?

'Definition' P the class of problems solvable in polynomial time

'Definition' NP the class of problems solvable in non-deterministic polynomial time.

i.e., guess the solution in O(1) time and verify in polynomial time.

- SAT, 3-SAT, Traveling Salesman Problem, Knapsack Problem, etc, are in NP

'Definition' H is NP-Hard if any NP problem can be reduced to H in polynomial time.

- SAT is NP-Hard

'Definition' H is NP-Complete if there exists a NP-Complete problem L that reduces in polynomial time to H.

- SAT is NP-Complete (S.A. Cook, ACM STOC, 1971)
- If there exists a polynomial time algorithm for any NP-Complete problem then P = NP.

See for a more formal introduction to the theory of NP-Completeness:
Michael R. Garey and David S. Johnson (1979).
Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman. ISBN 0-7167-1045-5.

A Short Introduction to Number Theory

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

15

Number Theory

Definition (Divisors):
b ≠ 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 Question: does -4 | 24 hold?

The following relations hold:

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

16

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:

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

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

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

17

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

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

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

18

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:

$74 = 2 \times 37$

$75 = 3 \times 5^2$

$gcd(74,75) = 1$

19

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: $a \equiv b \bmod n$

20

Number Theory: Modular Arithmetic

Examples: $73 \equiv 4 \bmod 23$ as

$73 = 3 \times 23 + 4$, hence

$(73 \bmod 23) = 4$, and clearly $4 = (4 \bmod 23)$, thus

$(73 \bmod 23) = (4 \bmod 23) \Rightarrow 73 \equiv (4 \bmod 23)$

$21 \equiv -9 \bmod 10$ 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 $a \equiv c \bmod n$

21

Number Theory: Modular Arithmetic

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

The following properties hold for modular arithmetic within $\mathbb{Z}_n$:

- $(w + x) \bmod n = (x + w) \bmod n$
- $((w+x)+y) \bmod n = (w+(x+y)) \bmod n$
- $(0+w) \bmod n = w \bmod n$
- $\forall w \in \mathbb{Z}_n \; \exists z \in \mathbb{Z}_n$ such that $w + z \equiv 0 \bmod n$

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

22

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 number z such that $w \times z \equiv 1 \bmod p$,

z is equal to the multiplicative inverse w^{-1} of w

23

Fast Exponentiation

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

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

I	b_i	Exponent c	result 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
```

24

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 all 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 to n. Thus $\Phi(n) = pq - (q-1) - (p-1) - 1 = (p-1)(q-1)$.

25

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, and m an integer such that gcd(m,n)=1, then

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

Examples:

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

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

26

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 $1 - 2^{-s}$.

27

Number Theory: Number of Primes

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

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.

28

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

Theorem: For any integer $a \ge 0$, 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

29

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

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

i.e., $dd^{-1} = 1 \bmod n$.

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

30

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^*.

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

31

- 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

$O(\log^2 n)$