Biomedical Security

Erwin M. Bakker

Some Security News

Backdoor Added — But Found — in PHP

Unknown hackers attempted to add a backdoor to the PHP source code. It was two malicious commits, with the subject "fix typo" and the names of known PHP developers and maintainers. They were discovered and removed before being pushed out to any users. But since 79% of the Internet's websites use PHP, it's scary.

Developers have moved PHP to GitHub, which has better authentication. Hopefully it will be enough — PHP is a juicy target.

Tags: authentication, backdoors, hacking, open source, supply chain

Posted on April 9, 2021 at 8:54 AM • 17 Comments

Like Tweet

From: schneier.com

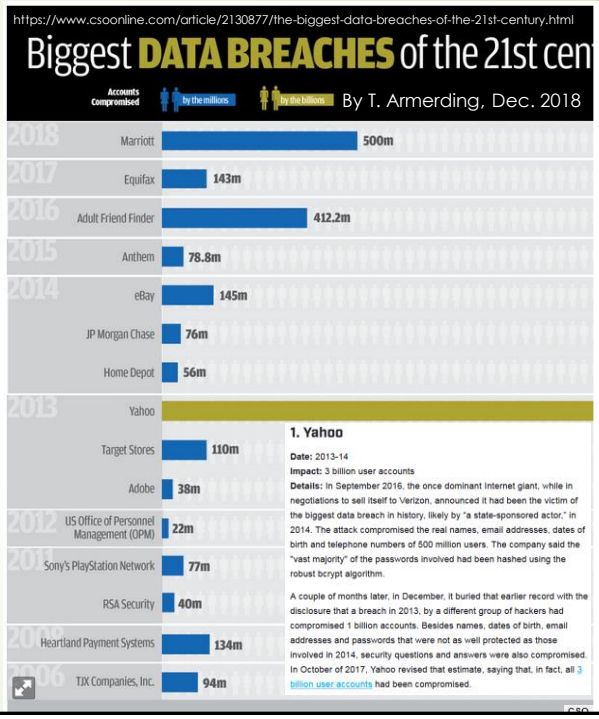
Datalek bij GGD: gegevens van miljoenen Nederlanders in criminele handen

De privégegevens van miljoenen Nederlanders uit de it-systemen die door de GGD worden gebruikt, worden illegaal op internet verhandeld. Wat zijn de risico's?

Laurens Verhagen 26 januari 2021, 14:10

From: Volkskrant

https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html



Overview

- Cryptography: Classical Algorithms,
- Cryptography: Public Key Algorithms
- Cryptography: Protocols
- Cryptography Workshop
- Biomedical Security and Applications
- Student Presentations

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

Cryptography: Sharing Secrets

Alice

$C = E_K$ ('HELLO BOB')

Secret key K

Crypto-text C

Bob

$D_K(C)$ = 'HELLO BOB'

Secret key K

K?

Eve

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!

Public Key Crypto Systems

Alice

$C = E_{Bob}$ ('HELLO BOB')

Get Public Key E_{Bob}
From Bob or
from Public Key Register

Crypto-text C

Public Key Register

E_{Bob}
E_{Alice}
E_{Eve}
E_{You}
…
E_{Me}

Bob

D_{Bob} (C) = 'HELLO BOB'

Secret Key D_{Bob}
Public Key E_{Bob}
Publish Public Key **E_{Bob}** on Public Key Register or send to Alice

Digital Signatures

Message M, **Signature S**

Public Key Register

E_{Bob}
E_{Alice}
E_{Eve}
E_{You}
…
E_{Me}

Alice

M = 'Message from Alice'
S = D_{Alice} ('Message from Alice')

Secret Key D_{Alice}
Public Key E_{Alice}
on Public Key Register, or send to Bob

Bob

Verify:
E_{Alice} (**S**) = 'Message from Alice' = M

Get Public Key E_{Alice}

Public Key Crypto System: RSA

*Rivest, R.; Shamir, A.; Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" . Communications of the ACM. **21** (2): 120–126. (Feb. 1978).*

- Key Generation
  - Select p, q, both primes.
  - Calculate $n = p * q$
  - Calculate $\varphi(n) = (p-1)(q-1)$
  - Select e such that $\gcd(\varphi(n), e) = 1$ and $1 < e < \varphi(n)$
  - Calculate d such that $d = e^{-1} \bmod \varphi(n)$
  - Public key is (e, n)
  - Secret key is (d, n)
- Encryption of plaintext $M < n$

  $C = M^e \bmod n$
- Decryption of ciphertext/crypto-text C

  $M = C^d \bmod n$

9

Are there enough 'big' 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

$$10^{100}/\ln(10^{100}) - 10^{99}/\ln(10^{99}) = 0.039 \times 10^{99}$$ 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.

10

How do we know a number is a Prime?

[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 $1 - 2^{-s}$.

Number Theory: Complexity of PRIMES

11

- Finding Primes
  - PRIMES: Let n be an integer. Is n prime?
  - PRIMES is in P, AKS-Algorithm, August 2002
  - **Finding a prime: expected success after ~1/115**
  - **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.**

Agrawal–Kayal–Saxena primality test and cyclotomic AKS test

Agrawal, Manindra; Kayal, Neeraj; Saxena, Nitin (2004). "PRIMES is in P" (PDF). Annals of Mathematics. 160 (2): 781–793. JSTOR 3597229. doi:10.4007/annals.2004.160.781.
The authors received the 2006 Gödel Prize and the 2006 Fulkerson Prize for this work.

Public Key Crypto System: RSA

*Rivest, R.; Shamir, A.; Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" . Communications of the ACM. **21** (2): 120–126. (Feb. 1978).*

- Key Generation

  Select p, q, both primes.
  Calculate $n = p * q$
  Calculate $\varphi(n) = (p-1)(q-1)$
  Select e such that $\gcd(\varphi(n), e) = 1$ and $1 < e < \varphi(n)$
  Calculate d such that $d = e^{-1} \bmod \varphi(n)$
  Public key is (e, n)
  Secret key is (d, n)

- Encryption of plaintext $M < n$

  $C = M^e \bmod n$

- Decryption of ciphertext/crypto-text C

  $M = C^d \bmod n$

13

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

14

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:

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

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

Public Key Crypto System: RSA

*Rivest, R.; Shamir, A.; Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" . Communications of the ACM. **21** (2): 120–126. (Feb. 1978).*

- Key Generation

  Select p, q, both primes.

  Calculate $n = p * q$

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

  Select e such that $\gcd(\varphi(n), e) = 1$ and $1 < e < \varphi(n)$

  Calculate d such that $d = e^{-1} \bmod \varphi(n)$

  Public key is (e, n)

  Secret key is (d, n)

- Encryption of plaintext $M < n$

  $C = M^e \bmod n$

- Decryption of ciphertext/crypto-text C

  $M = C^d \bmod n$

16

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

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

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

17

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:

$$74 = 2 \times 37$$
$$75 = 3 \times 5^2$$
$$\gcd(74,75) = 1$$

18

Number Theory: Euclid's Algorithm (~300 BC) 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
=> 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(18,12) = gcd(12, 18 mod 12) = gcd(12,6) = gcd(6, 12 mod 12) = gcd(6,0) = 6
- gcd(10,11) = gcd(11,10) = gcd(10, 11 mod 10) = gcd(10,1) = 1

19

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.

Public Key Crypto System: RSA

*Rivest, R.; Shamir, A.; Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" . Communications of the ACM. **21** (2): 120–126. (Feb. 1978).*

- Key Generation
  - Select p, q, both primes.
  - Calculate $n = p * q$
  - Calculate $\varphi(n) = (p-1)(q-1)$
  - Select e such that $\gcd(\varphi(n), e) = 1$ and $1 < e < \varphi(n)$
  - Calculate d such that $d = e^{-1} \bmod \varphi(n)$
  - Public key is (e, n)
  - Secret key is (d, n)
- Encryption of plaintext $M < n$

  $C = M^e \bmod n$
- Decryption of ciphertext/crypto-text C

  $M = C^d \bmod n$

21

Fast Exponentiation

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

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

I	bit 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
```

Public Key Crypto System: RSA

*Rivest, R.; Shamir, A.; Adleman, L. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" . Communications of the ACM. **21** (2): 120–126. (Feb. 1978).*

- Key Generation
  - Select p, q, both primes.
  - Calculate $n = p * q$
  - Calculate $\varphi(n) = (p-1)(q-1)$
  - Select e such that $\gcd(\varphi(n), e) = 1$ and $1 < e < \varphi(n)$
  - Calculate d such that $d = e^{-1} \bmod \varphi(n)$
  - Public key is (e, n)
  - Secret key is (d, n)
- Encryption of plaintext $M < n$

  $C = M^e \bmod n$
- Decryption of ciphertext/crypto-text C

  $M = C^d \bmod n$

Number Theory: FACTORIZE

23

- 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.

Public Key Crypto System: RSA Example

- Key Generation

  $p = 5, q = 11$

  => $n = p \times q = 5x11 = 55$ and $\varphi(n) = (p-1)(q-1) = 4x10 = 40$

  $e = 7$, is such that $\gcd(\varphi(n), e) = \gcd(40,7) = 1$ and clearly $1 < 7 < \varphi(n)$

  then $d = 23 = e^{-1} \bmod \varphi(n)$ as $(7x23 \bmod 24) = 161 \bmod 40 \equiv 1$

  Public key is $(7, 55)$

  Secret key is $(23, 55)$

- Encryption of plaintext $M = 2 < n = 55$

  $C = (M^e \bmod n) = (2^7 \bmod 55) = (128 \bmod 55) = 18 \bmod 55 \equiv 18$

- Decryption of ciphertext/crypto-text C

  now $C^d \bmod n = (18^{23} \bmod 55) = (2^{23}x3^{46} \bmod 55) = (4x18x18x18x3^6 \bmod 55) =$
  $(32 \times 3^{12} \bmod 55) = (32x26^3 \bmod 55) = (2x18x13^3 \bmod 55) = (79092 \bmod 55) =$
  $(1438x55 + 2 \bmod 55) = 2 \bmod 55 \equiv 2 = M$

RSA Chosen Ciphertext Attack

- Note for RSA: $E_e(M_1)xE_e(M_2) = E_e(M_1xM_2)$
- Assume (e,n) is the public keys and (d,n) the private key.
- Assume $C \equiv M^e \bmod n$ is intercepted.

Chosen Ciphertext attack:

- Compute $X \equiv (C \times 2^e) \bmod n$
- Submit X as a chosen ciphertext and receive back $Y \equiv X^d \bmod n$
- $X \equiv (C \times 2^e) \bmod n = (C \bmod n) \times (2^e \bmod n) = (M^e \bmod n) \times (2^e \bmod n) = (2M)^e \bmod n$
- Thus $Y \equiv X^d \bmod n = (2M)^{ed} \bmod n = 2M \bmod n$

Unsafe Modes of RSA

- Unsafe primes, etc.
- D. Boneh et al. Why Textbook ElGamal and RSA Encryption Are Insecure, T. Okamoto (Ed.): ASIACRYPT2000, LNCS 1976, pp. 30–43, 2000:
  - **without proper preprocessing of the plaintexts, both ElGamal and RSA encryption are fundamentally insecure.**
  - **when these systems encrypt a (short) secret key of a symmetric cipher it is often possible to recover the secret key from the ciphertext.**

  Conclusion: Preprocessing messages prior to encryption is an essential part of both systems.

Optimal Asymmetric Encryption Padding (**OAEP**)

Introduced by Bellare and Rogaway in 1994.

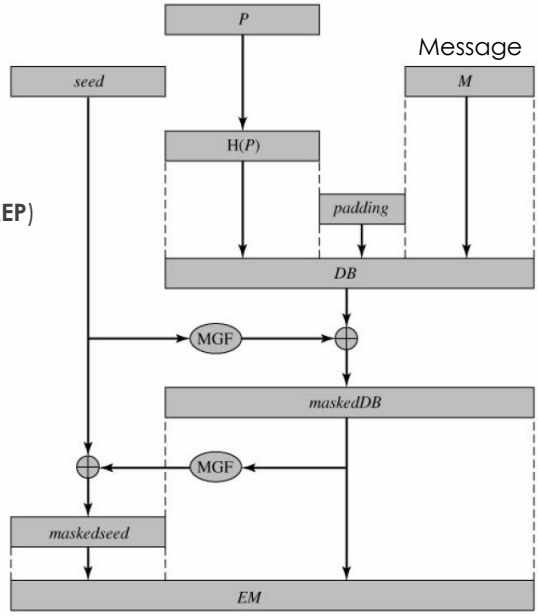
Safe Mode of RSA

Optimal Asymmetric Encryption Padding (**OAEP**)

Introduced by Bellare and Rogaway in 1994.

Note:
We can randomly pad the plaintext prior to encryption,
Then for this adapted version of RSA:
$\xi_e(M_1)x\,\xi_e(M_2) \neq \xi_e(M_1 x M_2)$, but this is not enough.

OAEP is a solution:
- P is a set of optional parameters.
- MGF is jus another hash function.
- EM is finally encoded using RSA.



Diffie-Hellman Key-Exchange based on difficulty of Discrete Log

28

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^*.

Diffie-Hellman Key-Exchange based on difficulty of Discrete Log

29

- Calculating the Discrete Logarithm
  - Assumed to be difficult.
  - If the prime factors of (p-1) are small there exist efficient algorithms, otherwise roughly the same complexity as factorising.

Diffie-Hellman Key Exchange Algorithm

- Global and Public

  Prime **q**, and $\alpha < q$ a primitive root of **q**,

  i.e., α generates the multiplicative group of integers **mod q**
- Alice Key Generation

  Select private $X_A < q$

  Calculate public $Y_A = \alpha^{X_A} mod\ q$
- Bob Key Generation

  Select private $X_B < q$

  Calculate public $Y_B = \alpha^{X_B} mod\ q$
- Generation of the Exchanged Secret Key by Alice

  $K = (Y_B)^{X_A} mod\ q$
- Generation of the Exchanged Secret Key by Bob

  $K = (Y_A)^{X_B} mod\ q$

Diffie-Hellman Key-Exchange Example

- α generates the multiplicative group of integers mod q

For example:

If $\alpha = 2, q = 7$, then α is **no** generator of $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ as

$\{2^0 \bmod 7, 2^1 \bmod 7, 2^2 \bmod 7, 2^3 \bmod 7, 2^4 \bmod 7, 2^5 \bmod 7\} = \{1, 2, 4, 1, 2, 4, 1\} \neq \mathbb{Z}_7^*$

If $\alpha = 3, q = 7$, then

$\{3^0 \bmod 7, 3^1 \bmod 7, 3^2 \bmod 7, 3^3 \bmod 7, 3^4 \bmod 7, 3^5 \bmod\} = \{1, 3, 2, 6, 4, 5\} = \mathbb{Z}_7^*$

Note: Assuming the generalized Riemann hypothesis, the least primitive root $\alpha_p = O(\log^6 p)$ (Shoup,1990, 1992).

- Alice Key Generation:

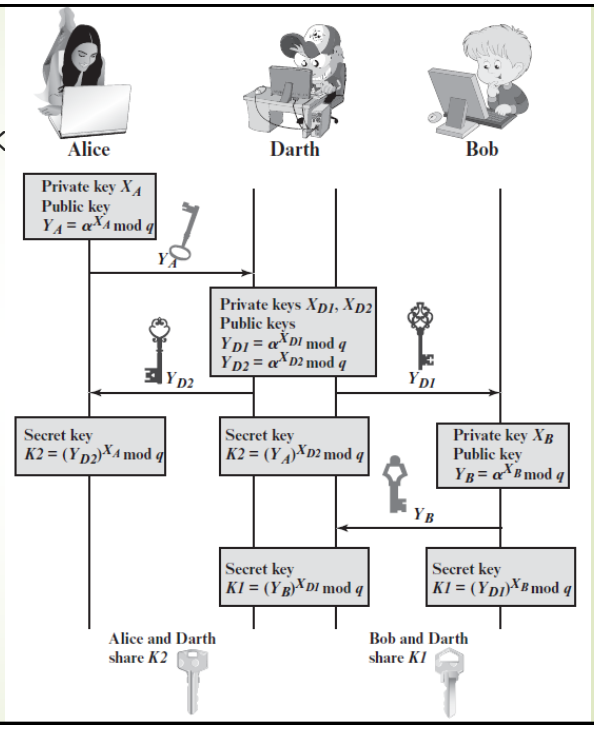
  Select private $X_A < q$

  Calculate public $Y_A = \alpha^{X_A} mod\ q$
- From Y_A it should be difficult to calculate X_A.
- Calculating X_A can be done taking the discrete log of Y_A to the base α modulo q

Diffie-Hellman Key Exchange Complexity of Discrete Log

- Calculating X_A by taking the discrete log of Y_A to the base α modulo q is **assumed** to be intractable.
- *Shor, Peter (1997). "**Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer**". SIAM Journal on Computing.* ***26*** *(5): 1484–1509.*
- *Adrian, David et al. (October 2015). "**Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice**":*
  - ***Logjam a flaw in TLS*** *that lets man-in-the middle downgrade connections to 'export-grade'-DH*
  - *Precomputations of a week for a 512-bit group => calculate discrete log for that group in ~ 1 minute.*
  - They found that 82% of vulnerable servers use a single 512-bit group, allowing us to compromise connections to 7% of Alexa Top Million HTTPS sites.
- **WeakDH.org: use a 2048-bit Diffie-Hellman group**

Diffie-Hellman Man-in-the-Middle Attack



Elliptic Curve Cryptography

Two main flavors:

- Prime curves over Z_p
- Binary curves over GF(2^m): Efficient implementations.

- Seems to use smaller keys for similar security level.
- Details are beyond scope of this course.
- In IEEE P1363 Standard for Public-Key Cryptography.

See A. Fernandes, 'Elliptic Curve Cryptography', Dr Dobb's Journal December 1999

Digital Signatures

Using a public key crypto system.

(M,S)

Alice

Bob

Message M and signature S

Checks using S if M is indeed from Alice

Digital Signatures

Using a public key crypto system.

(M,S)

Alice

Bob

Message M and signature $S = D_{Alice}(M)$

Checks with public E_{Alice}
if $E_{Alice}(S) = E_{Alice}(D_{Alice}(M)) = M$

Public Key Crypto System ElGamal

- Public Key
  - p a prime
  - $g < p$
  - $y = g^x mod\ p$
- Private Key
  - $x < p$
- Encryption of message M
  - random k, with $\gcd(k, p-1)=1$
  - $C = (a, b),\ where\ \ a = g^k mod\ p\ \ and\ \ b = y^k M\ mod\ p$
- Decryption
  - $M = b/a^x \bmod p = b.a^{-x} \bmod p$

ElGamal Signatures

- Public Key
  - p a prime
  - $g < p$
  - $y = g^x mod\ p$
- Private Key
  - $x < p$
- Signing of message M
  - random k, with $\gcd(k,p-1)=1$
  - Signature $S = (a, b),\ where$
  - $a = g^k mod\ p\ \ and\ \ b\ such\ that\ M = (xa + kb)\ mod\ p\text{-}1$
- Verification
  - Accept as valid if $y^a a^b\ mod\ p = g^M mod\ p$

39

Cryptographic Hash Functions

An **hash function** H has the following properties:

- H can be applied to data of any size.
- H produces fixed length output.
- H(x) is easy to compute for any given x.

- **One-way**

  for any given hash-code h, it is computationally infeasible to find x such that H(x) = h.
- **Weak collision resistance**

  for any given x, it is computationally infeasible to find y (not equal to x) such that H(y) = H(x).
- **Strong collision resistance**

  it is computationally infeasible to find any pair (x,y) such that H(x) = H(y).

40

Cryptographic Hash Functions

An **hash function** H has the following properties:

- H can be applied to data of any size.
- H produces fixed length output.
- H(x) is easy to compute for any given x.

- **One-way**

  for any given hash-code h, it is computationally infeasible to find x such that H(x) = h.
- **Weak collision resistance**

  for any given x, it is computationally infeasible to find y (not equal to x) such that H(y) = H(x).
- **Strong collision resistance**

  it is computationally infeasible to find any pair (x,y) such that H(x) = H(y).

Could you use DES to implement a Cryptographic Hash Function?

Secure Hash Algorithm (SHA)

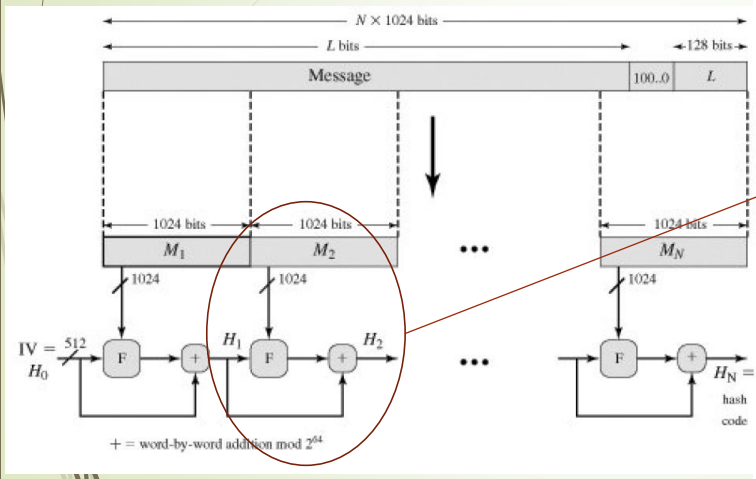
- Developed by NSA in 1993. Based on MD4.
- In 20002 a revised version by NIST. In 2005 SHA-1 started to be phased out by NIST. By 2010 SHA-256, SHA-384, and SHA-512.
- Around 2005 an attack were 2 different message could be found using 2^{69} operations yielding the same SHA-1 hash! (2^{80} operations were expected to be necessary)

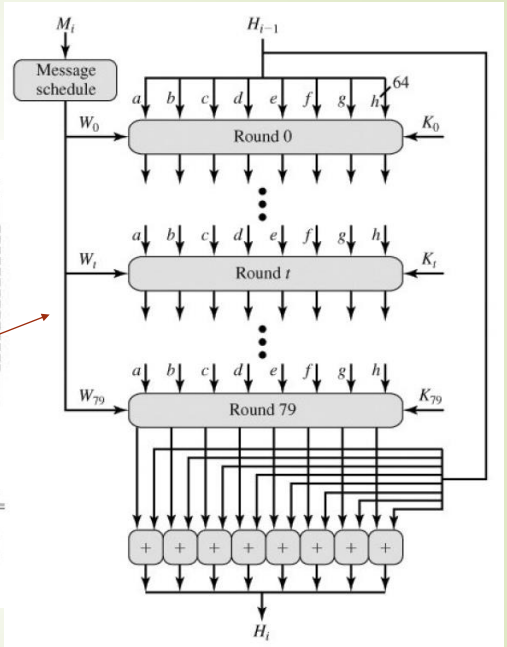
	SHA-1	SHA-256	SHA-384	SHA-512
Message digest size	160	256	384	512
Message size	$<2^{64}$	$<2^{64}$	$<2^{128}$	$<2^{128}$
Block size	512	512	1024	1024
Word size	32	32	64	64
Number of steps	80	64	80	80
Security	80	128	192	256

Notes: 1. All sizes are measured in bits.

2. Security refers to the fact that a birthday attack on a message digest of size *n* produces a collision with a workfactor of approximately $2^{n/2}$

Secure Hash Algorithm (SHA)





Assignment 3

- Find 1 (one !) research paper on (Biomedical) Security that you find very! Interesting and want to present during a 15 minutes talk.
- Send me the pdf of the paper **before** April 28th 2021, 23.59.

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 a and b are said to be congruent modulo n if
$(a \bmod n) = (b \bmod n)$

Notation: $a \equiv b \bmod n$

45

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 $a \equiv c \bmod n$

46

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 $w + z \equiv 0 \bmod n$

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

47

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 in Z_p^*

48

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^*.