CS5285
Information Security for eCommerce

Lecture 3

Prof. Gerhard Hancke
CS Department
City University of Hong Kong

Reminder of last week

- Symmetric Encryption
  - Substitution ciphers and frequency analysis
  - One time pad (perfectly secure/impractical)
  - Stream and block ciphers (RC4/DES/AES)
  - Block cipher modes of operation
    - Error propagation

Today's Lecture

- Number theory
  - Background maths to public key crypto
- CILO5

  (properties/design of security mechanisms)

Number Theory

We work on integers only

Divisors

Two integers: a and b (b is non-zero)

- b divides a if there exists some integer m such that $a = m \cdot b$
- Notation: $b|a$
- eg. 1,2,3,4,6,8,12,24 divide 24
- b is a **divisor** of a

Relations

1. If $b|1$ $\Rightarrow$ $b = \pm 1$
2. If $b|a$ and $a|b$ $\Rightarrow$ $b = \pm a$
3. If $b|0$ $\Rightarrow$ any $b \neq 0$
4. If $b|g$ and $b|h$ then $b \mid (mg + nh)$ for any integers m and n.

Congruence

a is **congruent** to b modulo n if $n \mid a-b$.

Notation: $a \equiv b \pmod{n}$

Examples

1. $23 \equiv 8 \pmod{5}$ because $5 \mid 23-8$
2. $-11 \equiv 5 \pmod{8}$ because $8 \mid -11-5$
3. $81 \equiv 0 \pmod{27}$ because $27 \mid 81-0$

Properties

1. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
2. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$

Modular Arithmetic

- **modular reduction:** $a \bmod n = r$

  r is the remainder when a is divided by a natural number n
- **r** is also called the residue of a mod n
  - it can be represented as: $a = qn + r$ where $0 \leq r < n$, $q = \lfloor a/n \rfloor$ where $\lfloor x \rfloor$ is the largest integer less than or equal to x
  - q is called the quotient
- 18 mod 7 = ?
- 29345723547 mod 2 = ?
- Relation between modular reduction and congruence
  - $-12 \equiv -5 \equiv 2 \equiv 9 \pmod 7$
  - -12 mod 7 = 2 (what's the quotient?)
  - $-12 = q*n+r= -2*7+2$

Modular Arithmetic Operations

- can do modular reduction at any point,
  - a + b mod n = [a mod n + b mod n] mod n
  - E.g. 97 + 23 mod 7 = [97 mod 7 + 23 mod 7] mod 7 = [6 + 2] mod 7 = 1
  - E.g. 11 – 14 mod 8 = ?

    3-6 mod 8 = 5
  - E.g. 11 x 14 mod 8 = ?

    3 x 6 mod 8 = 2

Prime and Composite Numbers

- An integer p is prime if its only divisors are ± 1 and $\pm p$ only.
- Otherwise, it is a composite number.
- E.g. 2,3,5,7 are prime; 4,6,8,9,10 are not
- List of prime numbers less than 200:

$2\ 3\ 5\ 7\ 11\ 13\ 17\ 19\ 23\ 29\ 31\ 37\ 41\ 43\ 47\ 53\ 59\ 61\ 67\ 71\ 73\ 79$
$83\ 89\ 97\ 101\ 103\ 107\ 109\ 113\ 127\ 131\ 137\ 139\ 149\ 151\ 157$
$163\ 167\ 173\ 179\ 181\ 191\ 193\ 197\ 199$

- Prime Factorization: If a is a composite number, then a can be factored in a unique way as

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$$

where $p_1 > p_2 > \dots > p_t$ are prime numbers and each α_i is a natural number (i.e. a positive nonzero integer).

e.g. $12{,}250 = 7^2 \cdot 5^3 \cdot 2$

Prime Factorization

- It is generally hard to do (prime) factorization when the number is large
- E.g. factorize
    1. 24070280312179
    2. 108930024809249102 51
    3. 938740932174981739832107481234871432497617
    4. 9387409321749817398321074812348714324976 1717

Greatest Common Divisor (GCD)

- GCD (a,b) of a and b is the largest number that divides both a and b
  - E.g. GCD(60,24) = 12
- If GCD(a, b) = 1, then a and b are said to be **relatively prime**
  - E.g. GCD(8,15) = 1
  - 8 and 15 are relatively prime (co-prime)

Question: How to compute gcd(a,b)?

Naive method: factorize a and b and compute the product of all their common factors.

e.g. $540 = 2^2 \times 3^3 \times 5$
$144 = 2^4 \times 3^2$
$\gcd(540, 144) = 2^2 \times 3^2 = 36$

Problem of this naive method: factorization becomes very difficult when integers become large.

Better method: Euclidean Algorithm (a.k.a. Euclid's GCD algorithm)

Euclidean Algorithm

Euclid's Algorithm:

```
A=a, B=b
while B>0
        R = A mod B
        A = B, B = R
return A
```

Rationale

Theorem $\gcd(a, b) = \gcd(a, b \bmod a)$

Compute gcd(911, 999) :

A	$= q \times B + R$
999	$= 1 \times 911 + 88$
911	$= 10 \times 88 + 31$
88	$= 2 \times 31 + 26$
31	$= 1 \times 26 + 5$
26	$= 5 \times 5 + 1$
5	$= 5 \times 1 + 0$

Value returned

Hence gcd(911, 999) = 1

Hence $\gcd(911, 999) = \gcd(911, 999 \bmod 911) = \gcd(911 \bmod 88, 88)$
$= \gcd(31, 88 \bmod 31) = \gcd(31 \bmod 26, 26) = \gcd(5, 26 \bmod 5)$
$= \gcd(5, 1) = 1.$

Modular Inverse

A is the modular inverse of B mod n if

AB mod n = 1.

A is denoted as B^{-1} mod n.

e.g.

- 3 is the modular inverse of 5 mod 7. In other words, 5^{-1} mod 7 = 3.
- 7 is the modular inverse of 7 mod 16. In other words, 7^{-1} mod 16 = 7.

However, there is no modular inverse for 8 mod 14.

There exists a modular inverse for B mod n if B is relatively prime to n.

Question:
What's the modular inverse of 911 mod 999?

Extended Euclidean Algorithm

The extended Euclidean algorithm can be used to solve the integer equation

$$ax + by = \gcd(a, b)$$

For any given integers a and b.

Example

Let a = 911 and b = 999. From the Euclidean algorithm,

$$\begin{aligned}
999 &= 1 \times 911 + 88 \\
911 &= 10 \times 88 + 31 \\
88 &= 2 \times 31 + 26 \\
31 &= 1 \times 26 + 5 \\
26 &= 5 \times 5 + 1 \qquad \Rightarrow \gcd(a, b) = 1
\end{aligned}$$

Tracing backward, we get

$$\begin{aligned}
1 &= 26 - 5 \times 5 \\
&= 26 - 5 \times (31 - 1 \times 26) = -5 \times 31 + 6 \times 26 \\
&= -5 \times 31 + 6 \times (88 - 2 \times 31) = 6 \times 88 - 17 \times 31 \\
&= 6 \times 88 - 17 \times (911 - 10 \times 88) = -17 \times 911 + 176 \times 88 \\
&= -17 \times 911 + 176 \times (999 - 1 \times 911) = \mathbf{176 \times 999 - 193 \times 911}
\end{aligned}$$

Calculating the Modular Inverse

we now have

$\gcd(911, 999) = 1 = -193 \times 911 + 176 \times 999.$

If we do a modular reduction of 999 to this equation, we have

$1 \pmod{999} = -193 \times 911 + 176 \times 999 \pmod{999}$
$\Rightarrow 1 = -193 \times 911 \bmod 999$
$\Rightarrow 1 = (-193 \bmod 999) \times 911 \bmod 999$
$\Rightarrow 1 = 806 \times 911 \bmod 999$

$1 \equiv 806 \times 911 \pmod{999}$.

Hence 806 is the **modular inverse** of 911 modulo 999.

The Euler phi Function

For $n \geq 1$, $\phi(n)$ denotes the number of integers in the interval $[1, n]$ which are relatively prime to n. The function ϕ is called the **Euler phi function** (or the **Euler totient function**).

Fact 1. The Euler phi function is multiplicative. I.e. if $gcd(m, n) = 1$, then $\phi(mn) = \phi(m) \times \phi(n)$.

Fact 2. For a prime p and an integer $e \geq 1$, $\phi(p^e) = p^{e-1}(p-1)$.

- From these two facts, we can find ϕ for any composite n if the prime factorization of n is known.
- Let $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ where $p_1,\dots, p_k$ are prime and each e_i is a nonzero positive integer.
- Then

$$\phi(n) = p_1^{e_1-1} (p_1-1) \,.\, p_2^{e_2-1} (p_2-1) \dots p_k^{e_k-1} (p_k-1)$$

The Euler phi Function

$$\phi(n) = \left|\{x : 1 \le x \le n \quad and \quad \gcd(x,n) = 1\}\right|$$

- $\phi(2) = |\{1\}| = 1$
- $\phi(3) = |\{1,2\}| = 2$
- $\phi(4) = |\{1,3\}| = 2$
- $\phi(5) = |\{1,2,3,4\}| = 4$
- $\phi(6) = |\{1,5\}| = 2$

- $\phi(37) = 36$
- $\phi(21) = (3-1)\times(7-1) = 2\times 6 = 12$

Fermat's Little Theorem

Let p be a prime. Any integer a not divisible by p satisfies $a^{p-1} \equiv 1 \pmod{p}$.

- We can generalize the Fermat's Little Theorem as follows. This is due to Euler.

  Euler's Generalization Let n be a composite. Then $a^{\phi(n)} \equiv 1 \pmod{n}$ for any integer a which is relatively prime to n.

- E.g. $a=3; n=10$; $\varphi(10)=4 \Rightarrow 3^4 \equiv 81 \equiv 1 \pmod{10}$
- E.g. $a=2; n=11$; $\varphi(11)=10 \Rightarrow 2^{10} \equiv 1024 \equiv 1 \pmod{11}$

Exercise: Compute $11^{1,073,741,823}$ mod 13.
Compute $11^{12}.11^{12}.11^{12}.11^{12}.....11^{3}$ mod 13 $\equiv 5 \pmod{13}$

Modular Exponentiation

Let Z = { …, -2, -1, 0, 1, 2, … } be the set of integers.

Let a, e, n $\in$ Z.

Modular exponentiation a^e mod n is defined as repeated multiplications of a for e times modulo n.

Method 1 : Repeated Modular Multiplication (as defined)

e.g. 11^{15} mod 13 $= \underline{11 \times 11} \times 11 \times 11 \times \ldots \times 11 \bmod 13$

$= \underline{4 \times 11} \times 11 \times \ldots \times 11 \bmod 13$

$= \underline{5 \times 11} \times \ldots \times 11 \bmod 13$

:

$= 5$

- performed 14 modular multiplications
- Complexity = O(e)
- What if the exponent is large?

Modular Exponentiation

Method 2 : *Square-and-Multiply Algorithm*

e.g. $11^{15} \bmod 13 = 11^{8+4+2+1} \bmod 13 = 11^8 \times 11^4 \times 11^2 \times 11 \bmod 13$ — (1)

- $11^2 = 121 \equiv 4 \pmod{13}$ — (2)
- $11^4 = (11^2)^2 \equiv (4)^2 \equiv 3 \pmod{13}$ — (3)
- $11^8 = (11^4)^2 \equiv (3)^2 \equiv 9 \pmod{13}$ — (4)

Put (2), (3) and (4) into (1) and *get*

$11^{15} \equiv 9 \times 3 \times 4 \times 11 \equiv 5 \pmod{13}$

- performed at most $2\lfloor \log_2 15 \rfloor$ modular multiplications
- Complexity = $O(\lg(e))$

Modular Exponentiation

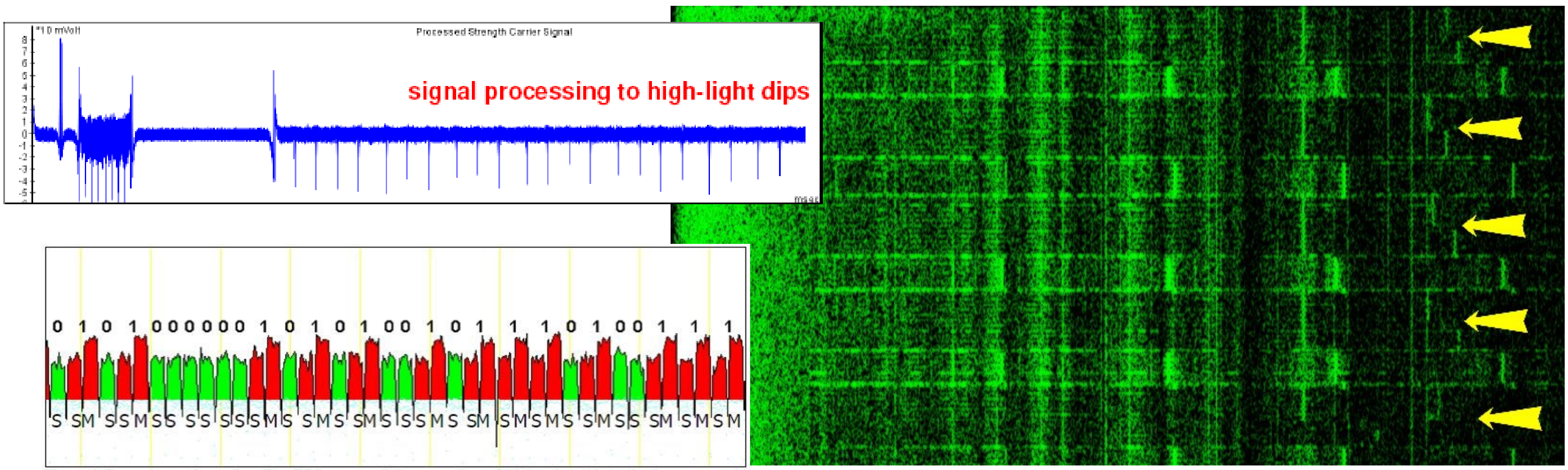
Pseudo-code of Square-and-Multiply Algorithm to compute $a^e \bmod n$:

Let the binary representation of e be $(e_{t-1}\ e_{t-2}\ \ldots\ e_1\ e_0)$.
Hence t is the number of bits in the binary representation of e.

```
z = 1
for i = t-1 downto 0 do
        z = z^2 mod n
        if e_i = 1 then z = z x a mod n
```

Side Channel

- Platform on which software runs leaks information
- Power usage, electromagnetic…acoustic
  - Consider again (square multiply) – timing?
  - Power (embedded hardware) and acoustic (PC, GNU RSA)



The end!

?

Any questions…

Exercise (Inverse)

e=79 and $e.d$ mod 3220 $\equiv$ 1 mod 3220 – find d
$d \equiv 79^{-1}$ mod 3220

Euclidean Algorithm
3220 = 40.79+60
79=1.60+19
60=3.19+3
19=6.3+1

Extended Euclidean Algorithm
1= 19-6.3
1= 19-6 (60-3.19) = -6.60+19.19
1= -6.60+19(79-1.60) = -25.60+19.79
1= -25(3220-40.79)+19.79 = 1019.79 -25.3220

1019.79 -25.3220 mod 3220 $\equiv$ 1019.79 mod 3220 $\equiv$ 1 mod 3220

Hence d = 1019 is the **modular inverse** of 79 modulo 3220.

Exercise 2 (Inverse)

Calculate 2084^{-1} mod 2357

Euclidean Algorithm

- 2357 = 1.2084 + 273
- 2084 = 7.273 + 173
- 273 = 1.173 + 100
- 173 = 1. 100 + 73
- 100 = 1.73+27
- 73=2.27+19
- 27=19+8
- 19=2.8+3
- 8=2.3+2
- 3=2+1

Exercise 2 (Inverse) ctd

- $1 = 3-1.2=3-(8-2.3) = 3.3-8$
- $3.(19-2.8)-8=3.19-7.8 = 3.19-7(27-19)=10.19-7.27$
- $10(73-2.27)-7.27 = 10.73-27.27 = 10.73 - 27(100-1.73) = 37.73-27.100$
- $37.73-27.100 = 37.(173-100)-27.100 = -64.100+37.173 = -64. (273-173)+37.173 = -64.273 +101.173$
- $-64.273 +101.173 = -64.273 +101.(2084-7.273) = -771.273+101.2084 = -771(2357-2084)+101.2084$
- $-771(2357-2084)+101.2084 = 872.2084-771.2357$
- $872.2084-771.2357 \bmod 2357 \equiv 872.2084 \bmod 2357 \equiv 1 \bmod 2357$
- So 872 must be modular inverse of 2084 mod 2357.

Exercise (Square/Mult)

Calculate 17^{130} mod 11

Powers of two? 1,2,4,8,16,32,64,128,256…
130 dec = 10000010 binary

$$17^{130} = 17^{128+2} \bmod 11 = 17^{128} \times 17^{2} \bmod 11$$

- $17^2 = 289 \equiv 3 \pmod{11}$ — (1)
- $17^4 = (17^2)^2 \equiv (3)^2 \equiv 9 \pmod{11}$ — (2)
- $17^8 = (17^4)^2 \equiv (9)^2 \equiv 4 \pmod{11}$ — (3)
- $17^{16} = (17^8)^2 \equiv (4)^2 \equiv 5 \pmod{11}$ — (4)
- $17^{32} = (17^{16})^2 \equiv (5)^2 \equiv 3 \pmod{11}$ — (5)
- $17^{64} = (17^{32})^2 \equiv (3)^2 \equiv 9 \pmod{11}$ — (6)
- $17^{128} = (17^{64})^2 \equiv (9)^2 \equiv 4 \pmod{11}$ — (7)

Use (7), (1) and get
$17^{130} \equiv 4 \times 3 \bmod 11 \equiv 1 \bmod 11$

Exercise 2 (Square/Mult)

Calculate 17^{170} mod 13

Powers of two? 1,2,4,8,16,32,64,128,256…

$17^{170} = 17^{128+32+8+2} \bmod 13 = 17^{128} \times 17^{32} \times 17^{8}\, 17^{2} \bmod 13$

- $17^2 = 289 \equiv 3 \pmod{13}$ — (1)
- $17^4 = (17^2)^2 \equiv (3)^2 \equiv 9 \pmod{13}$ — (2)
- $17^8 = (17^4)^2 \equiv (9)^2 \equiv 3 \pmod{13}$ — (3)
- $17^{16} = (17^8)^2 \equiv (3)^2 \equiv 9 \pmod{13}$ — (4)
- $17^{32} = (17^{16})^2 \equiv (9)^2 \equiv 3 \pmod{13}$ — (5)
- $17^{64} = (17^{32})^2 \equiv (3)^2 \equiv 9 \pmod{13}$ — (6)
- $17^{128} = (17^{64})^2 \equiv (9)^2 \equiv 3 \pmod{13}$ — (7)

Use (7), (5), (3), (1) and get
$17^{170} \bmod 13 \equiv 3 \times 3 \times 3 \times 3 \bmod 13 \equiv 3 \bmod 13$