

ECE 646 - Lecture 5

Mathematical Background: Modular Arithmetic

PGP Lab1: ID Card Due Today

GMU ID

Public Card

Name: GMU ECE 646

Email Address: gmuece646@gmail.com

Public Key Id: 0xDEC67765

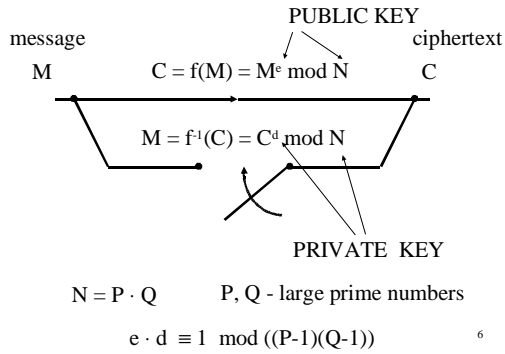
Finger Print: FDA0 9B76 E333 6E20 0417
0EC4 C823 A726 DEC6 7765



Motivation:

Public-key ciphers

RSA as a trap-door one-way function



RSA keys

PUBLIC KEY **PRIVATE KEY**

$\{ e, N \}$ $\{ d, P, Q \}$

$P, Q:$ P, Q - large prime numbers

$N:$ $N = P \cdot Q$

$e:$ $\gcd(e, P-1) = 1$ and $\gcd(e, Q-1) = 1$

$d:$ $e \cdot d \equiv 1 \bmod ((P-1)(Q-1))$

Mini-RSA keys

PUBLIC KEY **PRIVATE KEY**

$\{ e, N \}$ $\{ d, P, Q \}$

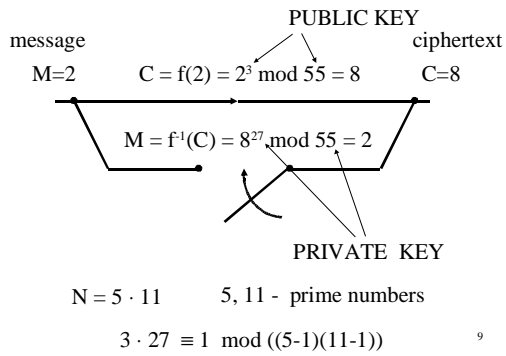
$P, Q:$ $P = 5$ $Q = 11$

$N:$ $N = P \cdot Q = 55$

$e:$ $\gcd(e, 5-1) = 1$ and $\gcd(e, 11-1) = 1$ $e=3$

$d:$ $3 \cdot d \equiv 1 \bmod 40$ $d=27$

Mini-RSA as a trap-door one-way function



Basic definitions

General Notation

\mathbb{Z} – integers

\exists - there exists

$\exists!$ - there exists unique

\forall - for all

\in - belongs to

\notin - does not belong to

Divisibility

$a \mid b$ a divides b
 a is a divisor of b

$a \mid b$ iff $\exists c \in \mathbb{Z}$ such that $b = c \cdot a$

$a \nmid b$ a does *not* divide b
 a is *not* a divisor of b

12

True or False?

$-3 \mid 18$ $14 \mid 7$ $7 \mid 63$ $-13 \mid 65$ $14 \mid 21$ $14 \mid 14$

$0 \mid 63$ $7 \mid 0$ $-5 \mid 0$ $0 \mid 0$

13

Prime vs. composite numbers

An integer $p \geq 2$ is said to be **prime** if its only *positive* divisors are 1 and p . Otherwise, p is called **composite**.

14

Prime or composite?

1 15 7 2 0 1 -13 103
1117 1239 1427

See

**“The Prime Pages: prime number research,
records, and resources”
by Chris Caldwell**

<http://www.utm.edu/research/primes/>

Greatest common divisor

Greatest common divisor of a and b , denoted by **$\gcd(a, b)$** ,
is the largest positive integer that divides both a and b .

$d = \gcd(a, b)$ iff

- 1) $d \mid a$ and $d \mid b$
- 2) if $c \mid a$ and $c \mid b$ then $c \leq d$

$\gcd(8, 44) =$

$\gcd(-15, 65) =$

$\gcd(45, 30) =$

$\gcd(31, 15) =$

$\gcd(0, 40) =$

$\gcd(121, 169) =$

Relatively prime integers

Two integers a and b are **relatively prime** or **co-prime**
if $\gcd(a, b) = 1$

18

Properties of the greatest common divisor

$$\gcd(a, b) = \gcd(a - kb, b)$$

for any $k \in \mathbf{Z}$

19

Quotient and remainder

Given integers a and n , $n > 0$

$\exists!$ $q, r \in \mathbf{Z}$ such that

$$a = q \cdot n + r \quad \text{and} \quad 0 \leq r < n$$

q – quotient

$$q = \left\lfloor \frac{a}{n} \right\rfloor = a \operatorname{div} n$$

r – remainder
(of a divided by n)

$$r = a - q \cdot n = a - \left\lfloor \frac{a}{n} \right\rfloor \cdot n = a \bmod n$$

20

$$1 \pmod{5} =$$

$$-32 \pmod{5} =$$

21

Integers congruent modulo n

Two integers a and b are **congruent modulo n**

(**equivalent modulo n**)

written $a \equiv b$

iff

$$a \pmod{n} = b \pmod{n}$$

or

$$a = b + kn, k \in \mathbb{Z}$$

or

$$n \mid a - b$$

22

Laws of modular arithmetic

23

Rules of addition, subtraction and multiplication modulo n

$$a + b \text{ mod } n = ((a \text{ mod } n) + (b \text{ mod } n)) \text{ mod } n$$

$$a - b \text{ mod } n = ((a \text{ mod } n) - (b \text{ mod } n)) \text{ mod } n$$

$$a \cdot b \text{ mod } n = ((a \text{ mod } n) \cdot (b \text{ mod } n)) \text{ mod } n$$

24

$$9 \cdot 13 \text{ mod } 5 =$$

$$25 \cdot 25 \text{ mod } 26 =$$

25

Laws of modular arithmetic

Regular addition

$$a+b = a+c$$

iff

$$b=c$$

Modular addition

$$a+b \equiv a+c \pmod{n}$$

iff

$$b \equiv c \pmod{n}$$

Regular multiplication

If $a \cdot b = a \cdot c$
and $a \neq 0$
then
 $b = c$

Modular multiplication

If $a \cdot b \equiv a \cdot c \pmod{n}$
and $\text{gcd}(a, n) = 1$
then
 $b \equiv c \pmod{n}$

26

Modular Multiplication: Example

$$18 \equiv 42 \pmod{8}$$

$$6 \cdot 3 \equiv 6 \cdot 7 \pmod{8}$$

$$3 \not\equiv 7 \pmod{8}$$

x	0	1	2	3	4	5	6	7
$6 \cdot x \pmod{8}$	0	6	4	2	0	6	4	2
x	0	1	2	3	4	5	6	7
$5 \cdot x \pmod{8}$	0	5	2	7	4	1	6	3

The Ring \mathbb{Z}_m

- Mathematical Structure
- Consists of:
 - The set $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$
 - Two operations “+” and “ \times ” for all $a, b \in \mathbb{Z}_m$ s.t.
 - $a + b \equiv c \pmod{m} (c \in \mathbb{Z}_m)$
 - $a \times b \equiv d \pmod{m} (d \in \mathbb{Z}_m)$

28

Properties of Rings

- Additive Identity** is the element zero “0”
 $a + 0 = a \pmod{m}$, for any $a \in \mathbb{Z}_m$
- Additive Inverse** “-a” of “a” is s.t.
 $a + (-a) \equiv 0 \pmod{m}$; $-a = m - a$ for any $a \in \mathbb{Z}_m$
- Addition is closed**: for any $a, b \in \mathbb{Z}_m$, $a + b \in \mathbb{Z}_m$
- Addition is commutative**: for any $a, b \in \mathbb{Z}_m$, $a + b = b + a$
- Addition is associative**: for any $a, b \in \mathbb{Z}_m$,
 $(a + b) + c = a + (b + c)$

29

Properties of Rings

- 1. Multiplicative Identity** is the element zero "1"
 $a \times 1 = a \text{ mod } m$, for any $a \in \mathbb{Z}_m$
- 2. Multiplicative Inverse** " a^{-1} " of " a " is s.t.
 $a \times a^{-1} \equiv 1 \text{ mod } m$; for any $a \in \mathbb{Z}_m$; Condition: $\text{gcd}(a,m)=1$
- 3. Multiplication is closed**: for any $a, b \in \mathbb{Z}_m$, $a \times b \in \mathbb{Z}_m$
- 4. Multiplication is commutative**: for any $a, b \in \mathbb{Z}_m$,
 $a \times b = b \times a$
- 5. Multiplication is associative**: for any $a, b \in \mathbb{Z}_m$,
 $(a \times b)c = a(b \times c)$

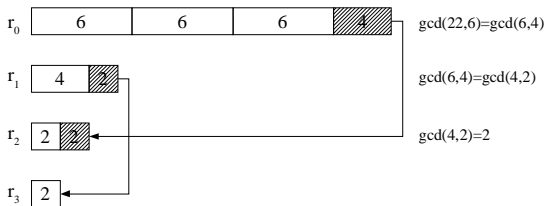
30

Algorithms

31

Euclid's Algorithm

- Compute $\text{gcd}(22,6)$



32

Euclid's Algorithm

Compute $\gcd(r_0, r_1)$; $r_0 > r_1$

index		
2	$r_0 = q_1 \cdot r_1 + r_2$	$\gcd(r_0, r_1) = \gcd(r_1, r_2)$
3	$r_1 = q_2 \cdot r_2 + r_3$	$\gcd(r_1, r_2) = \gcd(r_2, r_3)$
...
m	$r_{m-2} = q_{m-1} \cdot r_{m-1} + r_m$	$\gcd(r_{m-2}, r_{m-1}) = \gcd(r_{m-1}, r_m)$
	$r_{m-1} = q_m \cdot r_m + 0$	$\gcd(r_0, r_1) = \gcd(r_{m-1}, r_m) = r_m$

Termination Criteria

33

Euclid's Algorithm

Example: Compute $\gcd(973, 301)$; $r_0 > r_1$

index		
2	$r_0 = q_1 \cdot r_1 + r_2$	$973 = 3 \cdot 301 + 70$
3	$r_1 = q_2 \cdot r_2 + r_3$	$301 = 4 \cdot 70 + 21$
4	$r_2 = q_3 \cdot r_3 + r_4$	$70 = 3 \cdot 21 + 7$
5	$r_3 = q_4 \cdot r_4 + r_5$	$21 = 3 \cdot 7 + 0$

$\gcd(973, 301) = \gcd(21, 7) = 7$

Termination Criteria

34

Multiplicative inverse modulo n

The multiplicative inverse of a modulo n is an **integer [!!!]** x such that

$$a \cdot x \equiv 1 \pmod{n}$$

The multiplicative inverse of a modulo n is denoted by $a^{-1} \pmod{n}$ (in some books \bar{a} or a^*).

According to this notation:

$$a \cdot a^{-1} \equiv 1 \pmod{n}$$

35

Extended Euclidean Algorithm

Given r_0, r_1 , there exist s, t such that $s \cdot r_0 + t \cdot r_1 = \gcd(r_0, r_1)$; $r_0 > r_1$

index	Euclid's Algorithm	$r_j = s_j \cdot r_0 + t_j \cdot r_1$
2	$r_0 = q_1 \cdot r_1 + r_2$	$r_2 = r_0 - q_1 \cdot r_1 = s_2 \cdot r_0 + t_2 \cdot r_1$
3	$r_1 = q_2 \cdot r_2 + r_3$	$r_3 = r_1 - q_2 \cdot r_2 = r_1 - q_2(r_0 - q_1 \cdot r_1)$ $= [-q_2]r_0 + [1 + q_1 \cdot q_2]r_1$ $= s_3 \cdot r_0 + t_3 \cdot r_1$
...
i	$r_{i-2} = q_{i-1} \cdot r_{i-1} + r_i$	$r_i = s_i \cdot r_0 + t_i \cdot r_1$
...
m	$r_{m-2} = q_{m-1} \cdot r_{m-1} + r_m$	$r_m = \gcd(r_0, r_1) = s_m \cdot r_0 + t_m \cdot r_1$

Extended Euclidean Algorithm

• Recursive Formulae:

$$s_0 = 1, \quad t_0 = 0$$

$$s_1 = 0, \quad t_1 = 1$$

$$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}, \quad t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}; \quad i=2,3,4,\dots$$

• If $\gcd(r_0, r_1) = 1$, then $t = r_1^{-1} \pmod{r_0}$

Extended Euclidean Algorithm

Compute $20^{-1} \pmod{117}$; $r_0 = 117, r_1 = 20$

index	$r_{i-2} = q_{i-1} \cdot r_{i-1} + r_i$	q_{i-1}	$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$	$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$
2	$r_0 = 117 = 5 \cdot 20 + 17$	5	$s_2 = 1 - 5 \cdot 0 = 1$	$t_2 = 0 - 5 \cdot 1 = -5$
3	$r_1 = 20 = 1 \cdot 17 + 3$	1	$s_3 = 0 - 1 \cdot 1 = -1$	$t_3 = 1 - 1 \cdot (-5) = 6$
4	$r_2 = 17 = 5 \cdot 3 + 2$	5	$s_4 = 1 - 5 \cdot (-1) = 6$	$t_4 = -5 - 5 \cdot 6 = -35$
5	$r_3 = 3 = 1 \cdot 2 + 1$	1	$s_5 = -1 - 1 \cdot 6 = -7$	$t_5 = 6 - 1 \cdot (-35) = 41$

$r_3 = 1 = \gcd(117, 20)$, i.e., we are done; $20^{-1} \pmod{117} = t_5 = 41$
 Test: $20 \cdot 41 = 820 = 7 \cdot 117 + 1 = 1 \pmod{117}$

Extended Euclidean Algorithm

Compute $20^{-1} \bmod 117$; $r_0 = 117, r_1 = 20$

index	$r_{i-2} = q_{i-1} \cdot r_{i-1} + r_i$	q_{i-1}	$s_i = s_{i-2} - q_{i-1} \cdot s_{i-1}$	$t_i = t_{i-2} - q_{i-1} \cdot t_{i-1}$
2	$r_0 = 117 = 5 \cdot 20 + 17$	5	$s_2 = 1 - 5 \cdot 0 = 1$	$t_2 = 0 - 5 \cdot 1 = -5$
3	$r_1 = 20 = 1 \cdot 17 + 3$	1	$s_3 = 0 - 1 \cdot 1 = -1$	$t_3 = 1 - 1 \cdot -5 = 6$
4	$r_2 = 17 = 5 \cdot 3 + 2$	5	$s_4 = 1 - 5 \cdot -1 = 6$	$t_4 = -5 - 5 \cdot 6 = -35$
5	$r_3 = 3 = 1 \cdot 2 + 1$	1	$s_5 = -1 - 1 \cdot 6 = -7$	$t_5 = 6 - 1 \cdot -35 = 41$

$r_5 = 1 = \gcd(117, 20)$, i.e., we are done; $20^{-1} \bmod 117 = t_5 = 41$
 Test: $20 \cdot 41 = 820 = 7 \cdot 117 + 1 = 1 \bmod 117$

39

Motivation

Breaking ciphers

40

Historical ciphers

Affine Cipher

Key:

$$\text{Key} = (k_1, k_2) \quad k_1, k_2 \in [0, 25], \quad \gcd(k_1, 26) = 1$$

Encryption transformation:

$$c_i = f(m_i) = k_1 \cdot m_i + k_2 \bmod 26$$

Decryption transformation:

$$m_i = f^{-1}(c_i) = k_1^{-1} \cdot (c_i - k_2) \bmod 26$$

41

Coding characters into numbers

A \leftrightarrow 0	N \leftrightarrow 13
B \leftrightarrow 1	O \leftrightarrow 14
C \leftrightarrow 2	P \leftrightarrow 15
D \leftrightarrow 3	Q \leftrightarrow 16
E \leftrightarrow 4	R \leftrightarrow 17
F \leftrightarrow 5	S \leftrightarrow 18
G \leftrightarrow 6	T \leftrightarrow 19
H \leftrightarrow 7	U \leftrightarrow 20
I \leftrightarrow 8	V \leftrightarrow 21
J \leftrightarrow 9	W \leftrightarrow 22
K \leftrightarrow 10	X \leftrightarrow 23
L \leftrightarrow 11	Y \leftrightarrow 24
M \leftrightarrow 12	Z \leftrightarrow 25

42

Historical ciphers

Affine Cipher – Example (1)

Key:

Key = $(k_1, k_2) = (3, 11)$ $3, 11 \in [0, 25], \text{gcd}(3, 26)=1$

Encryption transformation:

$$c_i = f(m_i) = 3 \cdot m_i + 11 \pmod{26}$$

Decryption transformation:

$$k_1^{-1} = 3^{-1} \pmod{26} = 9 \quad \text{because} \quad 3 \cdot 9 \pmod{26} = 1$$

$$m_i = f^{-1}(c_i) = 9 \cdot (c_i - 11) \pmod{26}$$

43

Historical ciphers

Affine Cipher – Example (2)

	coding	encryption		decoding
N	\rightarrow 13	$\rightarrow 3 \cdot 13 + 11 \pmod{26} = 24$	\rightarrow	Y
S	\rightarrow 18	$\rightarrow 3 \cdot 18 + 11 \pmod{26} = 13$	\rightarrow	N
A	\rightarrow 0	$\rightarrow 3 \cdot 0 + 11 \pmod{26} = 11$	\rightarrow	L

44

Historical ciphers

Affine Cipher – Example (3)

coding decryption decoding

Y \longrightarrow 24 \longrightarrow $9 \cdot (24 - 11) \bmod 26 = 13 \longrightarrow$ N

N \longrightarrow 13 \longrightarrow $9 \cdot (13 - 11) \bmod 26 = 18 \longrightarrow$ S

L \longrightarrow 11 \longrightarrow $9 \cdot (11 - 11) \bmod 26 = 0 \longrightarrow$ A

45

Breaking the affine cipher (1)

Step 1: Establish a relative frequency of letters in the ciphertext

Ciphertext:

FMXVE DKAPH FERBN DKRXR SREFM ORUDS
DKDVS HVUFE DKAPR KDLYE VLRHH RH

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
=	-		≡	≡	≡	≡				≡	-	-	-	-	=		≡	≡	≡		≡	≡			

R	- 8
D	- 7
E, H, K	- 5

46

Most frequent single letters

Average frequency in a random string of letters:

$$\frac{1}{26} = 0.038 = 3.8\%$$

Average frequency in a long English text:

E	—	13%
T, N, R, I, O, A, S	—	6%-9%
D, H, L	—	3.5%-4.5%
C, F, P, U, M, Y, G, W, V	—	1.5%-3%
B, X, K, Q, J, Z	—	< 1%

47

Breaking the affine cipher (2)

Step 2: Assuming the relative frequency of letters in the corresponding message, derive the corresponding equations

Assumption: Most frequent letters in the message: E and T

Corresponding equations:

$$\begin{array}{ll} E \rightarrow R & f(E) = R \\ T \rightarrow D & f(T) = D \\ \\ 4 \rightarrow 17 & f(4) = 17 \\ 19 \rightarrow 3 & f(19) = 3 \end{array}$$

48

Breaking the affine cipher (3)

Step 3: Solving a set of equations for unknowns k_1 and k_2

$$\begin{array}{l} f(4) = 17 \\ f(19) = 3 \end{array}$$



$$\begin{array}{l} 4 \cdot k_1 + k_2 \equiv 17 \pmod{26} \\ 19 \cdot k_1 + k_2 \equiv 3 \pmod{26} \end{array}$$



$$15 \cdot k_1 \equiv -14 \pmod{26}$$



$$15 \cdot k_1 \equiv 12 \pmod{26}$$

49

Solving equations of the form $a \cdot x \equiv b \pmod{n}$ (linear congruences)

The equation

$$a \cdot x \equiv b \pmod{n}$$

has

1. one solution iff $\gcd(a, n) = 1$
 $x = a^{-1} \cdot b \pmod{n}$

2. no solutions iff $d = \gcd(a, n) \neq 1$, and $d \nmid b$

3. d solutions iff $d = \gcd(a, n) \neq 1$, and $d \mid b$
The solutions are

$x_0, x_0 + n/d, x_0 + 2 \cdot n/d, x_0 + 3 \cdot n/d, \dots, x_0 + (d-1) \cdot n/d,$
where $x_0 = (a/d)^{-1} \cdot (b/d) \pmod{n/d}$

50
