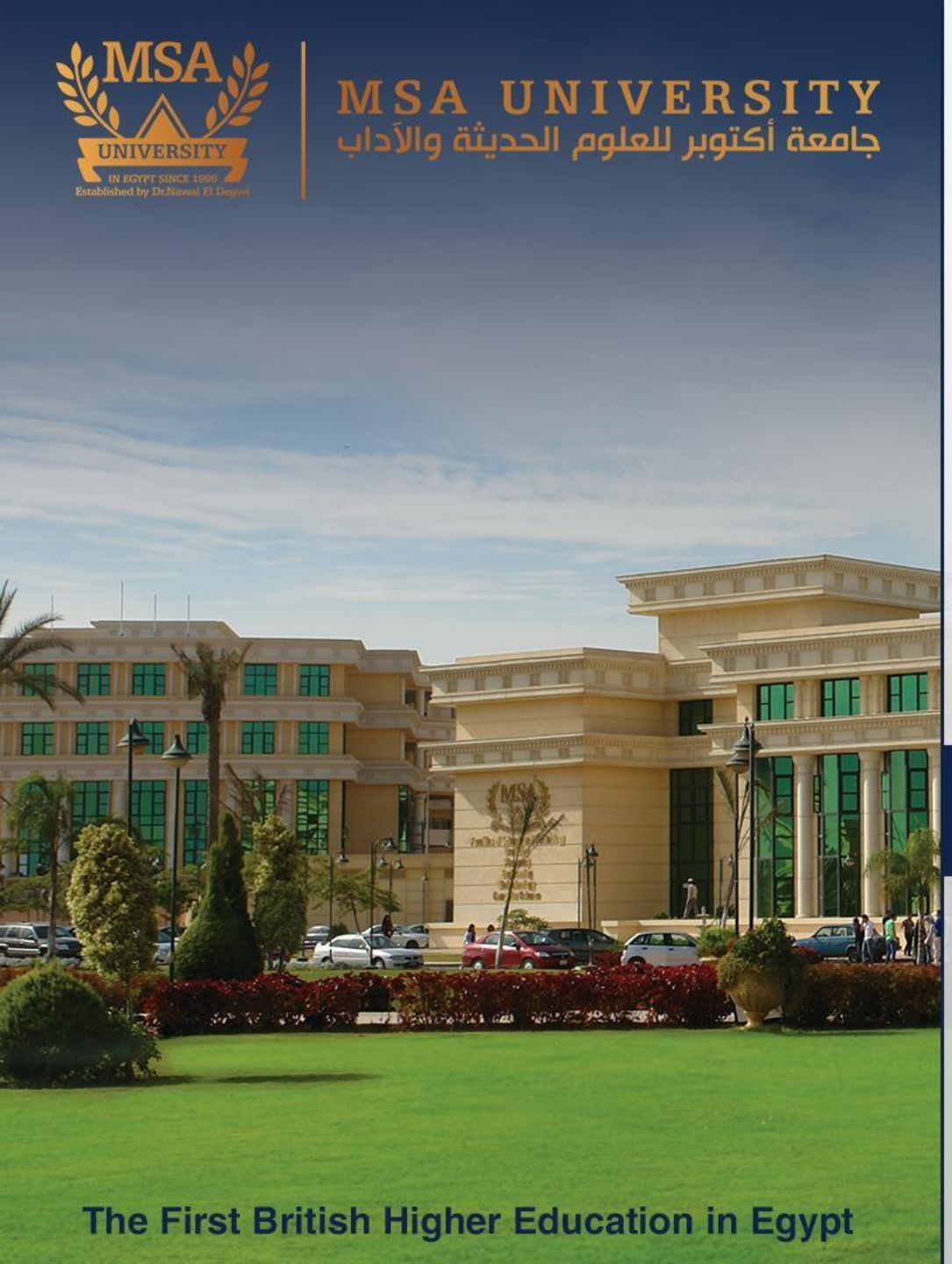


Cryptography
ECE5632 - Spring 2024

Lecture 2A

Dr. Farah Raad

Lecture Topic

Modular Arithmetic and More Historical Ciphers

Short Introduction to Modular Arithmetic

Why do we need to study modular arithmetic?

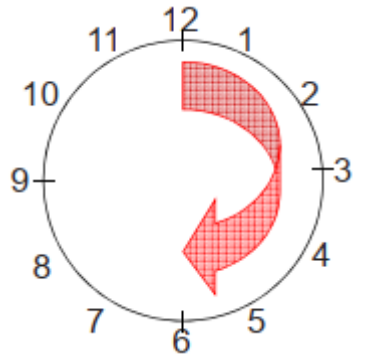
- Extremely important for asymmetric cryptography (RSA, elliptic curves etc.)
- Some historical ciphers can be elegantly described with modular arithmetic (Caesar and affine cipher).

Short Introduction to Modular Arithmetic

- Generally speaking, most cryptosystems are based on **sets of numbers** that are
  1. discrete (sets with integers are particularly useful)
  2. finite (i.e., if we only compute with a finely many numbers)

Seems too abstract? --- Let‘s look at a finite set with discrete numbers we are quite familiar with: a clock.
Consider the hours on a clock. If you keep adding one hour, you obtain:

1h,2h,3h,...,11h,12h,1h,2h,3h,...,11h,12h,1h,2h,3h,...



✓ Even though we keep adding one hour, we never leave the set.

Short Introduction to Modular Arithmetic

- We develop now an arithmetic system which allows us to **compute** in finite sets of integers
- It is crucial to have an operation which keeps the numbers within limits“, i.e., after addition and multiplication they should never leave the set .

Let’s look at a general way of dealing with arithmetic in such finite sets.
Example :* We consider the set of the nine numbers: *{*0,1,2,3,4,5,6,7,8*}

We can do regular arithmetic as long as the results are smaller than 9. For instance:
$2 \times 3 = 6$ & $4+4 = 8$
But what about 8+4?
Since 8+4 = 12, and 12/9 has a remainder of 3, we write: **$8+4 \equiv 3 \bmod 9$**

Modulus Operation

Definition: Modulus Operation

Let *a, r, m* be integers and *m* > 0. We write

a* ≡ *r* mod *m

if (*a-r) is divisible by m. >>> m/(a-r)= integer*

- "*m*" is called the **modulus**
- "*r*" is called the **remainder**

x mod n = r
a mod m = r

❖ *(≡) is mean the reading of equation be (a mod m equal r)*

Examples for modular reduction.

- Let a= 12 and m= 9 : 12 ≡ 3 mod 9
- Let a= 34 and m= 9: 34 ≡ 7 mod 9
- Let a= -7 and m= 9: -7 ≡ *2* mod 9

✓ (you should check whether the condition *m* divides (*r-a*) holds in each of the 3 cases)

Modulus Operation

Computation of the Remainder

$$a = q \cdot m + r \qquad \text{for } 0 \le r < m$$

Since; $a - r = q \cdot m$ (m divides $a-r$)

$$r = a - q \cdot m$$

we can now write: $a \equiv r \bmod m$

✓ Note that $r \in \{0,1,2,\ldots,m-1\}$.

Example: **Let $a = 42$ and $m = 9$.**

Then 42 = 4*9+6 and therefore 42 ≡ 6 mod 9.

Properties of Modular Arithmetic (1)

➢ The Remainder Is Not Unique

It is somewhat surprising that for every given modulus *m* and number *a*, there are (infinitely) many valid remainders.

$$r = a \pm m$$

Example: **We want to reduce 12 modulo 9. Here are several results which are correct according to the definition:**

- 12 ≡ 3 mod 9 → 3 is a valid remainder since 9 / (3-12) >>>> 12-9=3
- 12 ≡ 21 mod 9 → 21 is a valid remainder since 9 / (21-12) >>>> 12+9=21
- 12 ≡ -6 mod 9 → -6 is a valid remainder since 9 / (-6-12) >>>> 12-9=3 - 9= - 6

➢ "*x*|*y*" means "*x* divides *y*". There is a system behind this behavior. The set of numbers

{...,-24,-15,-6,3,12,15,24,...}

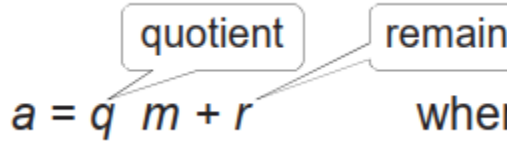
➢ There are eight other equivalence classes for the modulus 9 (*equivalence class)*

{...,-27,-18,-9, 0, 9,18,27,...}
{...,-26,-17,-8, 1, 10,19,28,...}
...
{...,-19,-10,-1, 8, 17,26,35,...}

Properties of Modular Arithmetic (2)

➢ Which remainder do we choose?

By convention, we usually agree on the **smallest positive integer *r*** as remainder. This integer can be computed as



- Example: *a=12* and *m= 9*

$$12 = 1 \times 9 + 3 \quad \rightarrow \quad r = 3$$

✓ Remark: This is just a convention. Algorithmically we are free to choose any other valid remainder to compute our crypto functions.

Properties of Modular Arithmetic (3)

➢ How do we perform modular division?

First, note that rather than performing a division, we prefer to multiply by the inverse.

$$b / a \equiv b \times a^{-1} \bmod m$$

The inverse a^{-1} of a number *a* is defined such that:

$$a \times a^{-1} \equiv 1 \bmod m$$

Ex: What is *5 / 7 mod 9* ?

The inverse of *7 mod 9* is *4* since *7 x 4 ≡ 28 ≡ 1 mod 9,* hence:

5 / 7 ≡ 5 x 4 = 20 ≡ 2 mod 9

Properties of Modular Arithmetic (4)

➢ Modular reduction can be performed at any point during a calculation

Let's look first at an example. We want to compute $3^8 mod\ 7$ (note that exponentiation is extremely important in public-key cryptography).

1. Approach: Exponentiation followed by modular reduction

$$3^8 = 6561 \equiv 2 \bmod 7$$

✓ Note that we have the intermediate result 6561 even though we know that the final result can't be larger than 7.

2. Approach: Exponentiation with intermediate modular reduction

$$3^8 = 3^4 \times 3^4 = 81 \times 81$$

At this point we reduce the intermediate results 81 modulo 7:

$$3^8 = 81 \times 81 \equiv 4 \times 4 \bmod 7$$
$$4 \times 4 = 16 \equiv 2 \bmod 7$$

General rule: For most algorithms it is advantageous to reduce intermediate results as soon as possible.

Integer Rings

➢ An Algebraic View on Modulo Arithmetic: The Ring *Zm* (1)

We can view modular arithmetic in terms of sets and operations in the set. By doing arithmetic modulo *m* we obtain **the integer ring *Zm*** .with the following properties:

- **Closure**: We can add and multiply any two numbers and the result is always in the ring.
- Addition and multiplication are **associative**, i.e., for all $a,b,c \varepsilon Z_m$

  $a + (b + c) = (a + b) + c$

  $a \times (b \times c) = (a \times b) \times c$

  and addition is **commutative**: $a + b = b + a$
- The **distributive law** holds: $a \times (b+c) = (a \times b) + (a \times c)$ for all $a,b,c \varepsilon Z_m$
- There is the **neutral element *0* with respect to addition**, i.e., for all $a \varepsilon Z_m$

  $a + 0 \equiv a \bmod m$
- For all $a \varepsilon Z_m$, there is always an **additive inverse element –*a*** such that

  $a + (-a) \equiv 0 \bmod m$
- There is the **neutral element 1 with respect to multiplication**, i.e., for all $a \varepsilon Z_m$

  $a \times 1 \equiv a \bmod m$
- The **multiplicative inverse a^{-1}**

  $a \times a^{-1} \equiv 1 \bmod m$

  exists only for some, but not for all, elements in Z_m.

Integer Rings

➢ An Algebraic View on Modulo Arithmetic: The Ring *Zm* (2)

Roughly speaking, a ring is a structure in which we can always add, subtract and multiply, but we can only divide by certain elements (namely by those for which a multiplicative inverse exists).

Ex: We consider the ring $Z_9 = \{0,1,2,3,4,5,6,7,8\}$

The elements 0, 3, and 6 do not have inverses since they are not coprime to 9.

The inverses of the other elements 1, 2, 4, 5, 7, and 8 are:

$1^{-1} \equiv 1 \bmod 9$ $\quad 2^{-1} \equiv 5 \bmod 9$ $\quad 4^{-1} \equiv 7 \bmod 9$

$5^{-1} \equiv 2 \bmod 9$ $\quad 7^{-1} \equiv 4 \bmod 9$ $\quad 8^{-1} \equiv 8 \bmod 9$

Integer Rings

➢ **Notes**

1. Mathematical operation ■ »»» (+, −, ∗ , /, exp)

$$X \blacksquare Y \bmod m = r$$

$$[\, X \bmod m \blacksquare Y \bmod m \,] \bmod m = r$$

Example: 7 + 8 mod 4 = [7 mod 4 + 8 mod 4] mod 4 = [3 + 0] mod 4 = 3

2. if a < m □r = a **Not need for Computation**

Example: 3 = r mod 8 □ r = 3

3. –a = r mod m a is –ve □ r = -a + m

Example: -3 = r mod 10 r = -3+ 10 = 7

4. a= r mod a m = a □ r = 0

Example: 10 = r mod 10 r = 0

More Historical Ciphers

- Two historical ciphers to introduce modular arithmetic with integers.
- A very popular special case of the substitution cipher is the **Caesar cipher and Affine Cipher.**

Shift (or Caesar) Cipher

- Ancient cipher, allegedly used by Julius Caesar to communicate with his army.
- Replaces each plaintext letter by another one. It is simply shifts the letters in the alphabet by a constant number of steps.

Let k, x, y ε {0,1, …, 25}

- Encryption: $y = e_k(x) \equiv x + k \bmod 26$
- Decryption: $x = d_k(x) \equiv y - k \bmod 26$

- Replacement rule is very simple: Take letter that follows after *k* positions in the alphabet
  Needs mapping from letters → numbers:

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

Shift (or Caesar) Cipher

Example Let the key be $k = 17$, and the plaintext is:

$$\texttt{ATTACK} = x_1, x_2, \ldots, x_6 = 0, 19, 19, 0, 2, 10.$$

The ciphertext is then computed as

$$y_1, y_2, \ldots, y_6 = 17, 10, 10, 17, 19, 1 = \texttt{rkkrtb}$$

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

Is the shift cipher secure?

No! several attacks are possible, including:

- Exhaustive key search (key space is only 26!)
- Letter frequency analysis, similar to attack against substitution cipher

Affine Cipher

- Extension of the shift cipher: rather than just adding the key to the plaintext, we also multiply by the key
- We use for this a key consisting of two parts: k = (a, b)

Let k, x, y ε {0,1, …, 25}

- Encryption: $y = e_k(x) \equiv a\,x + b \bmod 26$
- Decryption: $x = d_k(x) \equiv a^{-1}(y - b) \bmod 26$

The decryption is easily derived from the encryption function:

$a \cdot x + b \equiv y \bmod 26$

$a \cdot x \equiv (y - b) \bmod 26$

$x \equiv \boldsymbol{a}^{-1} \cdot (y - b) \bmod 26$

$a \times a^{-1} \equiv 1 \bmod 26$

Affine Cipher

Example Let the key be $k = (a, b) = (9, 13)$, and the plaintext be

$$\texttt{ATTACK} = x_1, x_2, \ldots, x_6 = 0, 19, 19, 0, 2, 10.$$

The inverse a^{-1} of a exists and is given by $a^{-1} = 3$. The ciphertext is computed as

$$y_1, y_2, \ldots, y_6 = 13, 2, 2, 13, 5, 25 = \texttt{nccnfz}$$

Let k, x, y ε {0,1, …, 25}

- Encryption: $y = e_k(x) \equiv a\,x + b \bmod 26$
- Decryption: $x = d_k(x) \equiv a^{-1}(y - b) \bmod 26$

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

Is the affine cipher secure?

No! The key space is only a bit larger than in the case of the shift cipher:

key space = (#values for a)×(#values for b)
= 12×26 = 312

- Again, several attacks are possible, including:
  - Exhaustive key search and letter frequency analysis, similar to the attack against the substitution cipher

MSA UNIVERSITY
IN EGYPT SINCE 1996
Established by Dr.Nawal El Degwi
MSA UNIVERSITY
جامعة أكتوبر للعلوم الحديثة والآداب

Thank You!

See You next Lectures!!
Any Question?

26th July Mehwar Road Intersection with Wahat Road, 6th of October City, Egypt
Tel: +202383711146 **Fax:** +20238371543 **Postal code:** 12451
Email: info@msa.eun.eg **Hotline:** 16672 **Website:** www.msa.edu.eg