DIVISIBILITY
MODULAR ARITHMETIC

Properties of Integers

Fractions – Terminology and Vocabulary

a rational number

$$\frac{245}{3}$$

245 ⇐ numerator

3 ⇐ denominator

$$a = k \times b + r$$

$$245 = 81 \times 3 + 2$$

dividend quotient divisor remainder

$$3\,\overline{)\,245}\quad 81 \text{ r } 2$$

$$245 \div 3 = 81 \text{ r } 2$$

$$a = k \times b + r$$

Dividend $a \in \mathbb{Z}$	Divisor $b \in \mathbb{Z}^+$	Quotient $k \in \mathbb{Z}$	Remainder $r \in \mathbb{N}$ and $0 \le r < b$
245	3		
41	8		
-99	11		
2	10		
-17	7		

Modulo function $a/b \Rightarrow a = k \times b + r$

The **quotient** k is commonly referred to as the integer part of the division. It is what is returned in an **integer division** operation.

The **modulo** or **mod-n** function returns the **remainder** r when a is divided by b. Ex. 12 mod 9 = 3 and 245 mod 81 = 2.

If $r=0$ then a is a **multiple of** b, or b **divides** a, written $b \mid a$, otherwise $b \nmid a$

Common usage in programming ⇒ quotient or integer division → $k = a / b$
remainder or mod n function → $r = a \% b$

WORKED EXAMPLES

Calculate the following modulo

- 7558 mod 63
- 7562 mod 63
- -7558 mod 63

WORKED EXAMPLES

What is (2500 + 1555 + 222 + 4) mod 5 ?

(a + b) **mod** n = ((a **mod** n) + (b **mod** n)) **mod** n

WORKED EXAMPLES

What is $(12 \times 13 \times 29 \times 69) \bmod 11$?

(ab) **mod** n = ((a **mod** n)(b **mod** n)) **mod** n

WORKED EXAMPLES

What is the remainder when $1! + 2! + 3! \ldots + 49!$ is divided by 20?

PRACTICE PROBLEMS

Without a calculator, calculate the following:

- $(123 + 234 + 32 + 56 + 22) \bmod 3$
- $(1594 \times (-117) \times 475) \bmod 6$
- $((-907) \times 17 \times (-276)) \bmod 15$
- $(43534569812031 \times 12903958235485) \bmod 2$

PRACTICE PROBLEMS

What is the remainder when $1! + 2! + 3! \ldots 100!$ is divided by 18?

If the remainder is 7 when positive integer n is divided by 18, what is the remainder when n is divided by 6?

PRACTICE PROBLEMS

- Using the 12-hour clock format, the current time is 4 o'clock, what time will it be 101 hours from now?

- Using the 12-hour clock format, the current time is 4 o'clock, what time was it 101 hours before?

PRACTICE PROBLEMS

- Given that February 14, 2018, is a Wednesday, what day of the week will February 14, 2090 be? Hint: take into account leap years.

WORKED EXAMPLES

Calculate 7^{358} mod 10.

k	7^k	7^k mod 10	
0			
1			
2			
3			
4			
5			
6			
7			
8			
9			

Modular arithmetic and cyclicity of remainders

Calculate 7^{358} mod 10.

What is the ones digit of 7^{358} ?

Same question, asking differently!

k	7^k	7^k mod 10	
0	1		
1	7		
2	49		
3	343		
4	2,401		
5	16,807		
6	117,649		
7	823,543		
8			
9			

Modular arithmetic and cyclicity of remainders

Base number ending with	Powers: seq of **ones** digit	Period of the cycle
0	0	1
1	1	1
2	2 4 8 6	4
3	3 9 7 1	4
4	4 6	2
5	5	1
6	6	1
7	7 9 3 1	4
8	8 4 2 6	4
9	9 1	2

- **Find remainders of large numbers**
  - ❑ Find the remainder of a^b mod 10
  - ❑ Find the ones digit of a^b
- When solving problems: try it and see if the **pattern** emerges, then use modulo to find the answer
- Also apply to the remainder of …
  - ❑ **mod 100**, i.e., find the tens digit
  - ❑ **other mod** ($\neq$10, $\neq$100)

Modular arithmetic and cyclicity of remainders

Base number ending with	Powers: seq of **tens** digit	Period of the cycle
0	0	1
1	0	1
2	…	20
3	…	20
4	…	10
5	2	1
6	3 1 9 7 5	5
7	0 0 4 4	4
8	…	20
9	…	10

- **Find remainders of large numbers**
  - ❑ **mod 100**, i.e., find the tens digit

o Know how to answer questions:

Asking for **the tens digit**
→ answer: a single digit 0-9

Asking for **mod 100**
→ find both tens & units digits
→ answer: a two-digit number
(or one-digit if it is less than 10)

WORKED EXAMPLES

- What is the tens digits of 7^{358} ?

k	7^k		
0			
1			
2			
3			
4			
5			
6			
7			
8			
9			

Hint: follow the same process as before, work on the tens instead of the ones digit

WORKED EXAMPLES

- What is the **tens digits** of 7^{358} ?

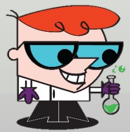
Same question, asking differently!

- Calculate 7^{358} **mod 100**.

k	7^k	tens digit	k mod 4
0			
1			
2			
3			
4			
5			
6			
7			
8			
9			

PRACTICE PROBLEMS

- Calculate 7^{355} mod 100.



Use the result of 7^{358} mod 100 from the last example to answer this (no need to re-calculate the cycles of both the ones & tens digits. Think divisibility & modulo!

PRACTICE PROBLEMS

- Find the tens digits of $6^{2345789}$

PRACTICE PROBLEMS

Calculate 4^{1000} mod 10.

PRACTICE PROBLEMS

It does not have to always be mod 10 or mod 100

- What is the remainder when 4^{1000} is divided by 7?

modulo of 7

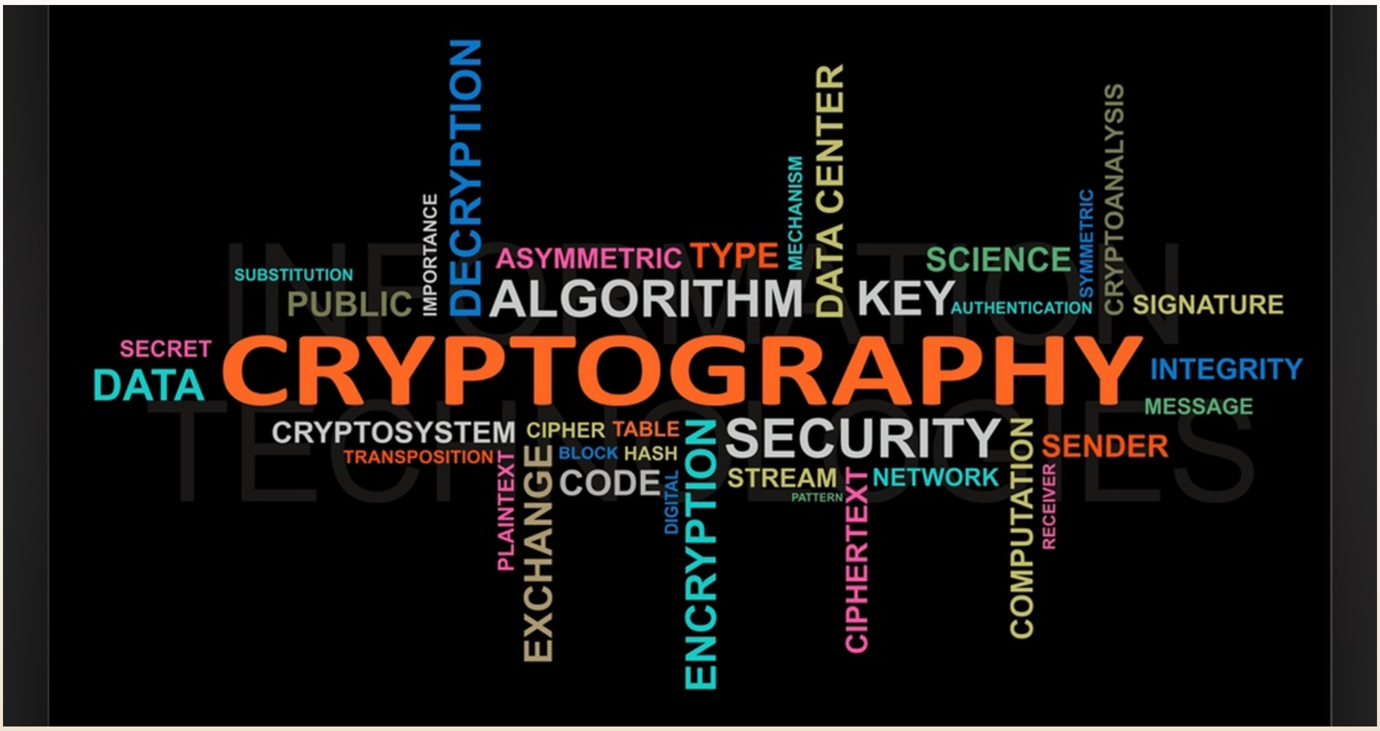
Hint: find a cyclic pattern of modulo 7 of powers of 4

PRACTICE PROBLEMS

It does not have to always be mod 10 or mod 100

- Calculate 7^{5140} mod 4.

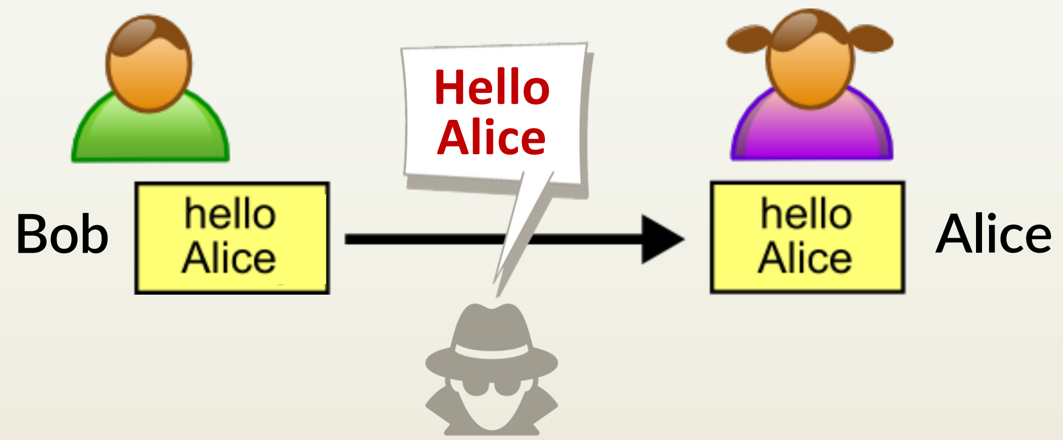
Hint: find a cyclic pattern of modulo 4 of powers of 7



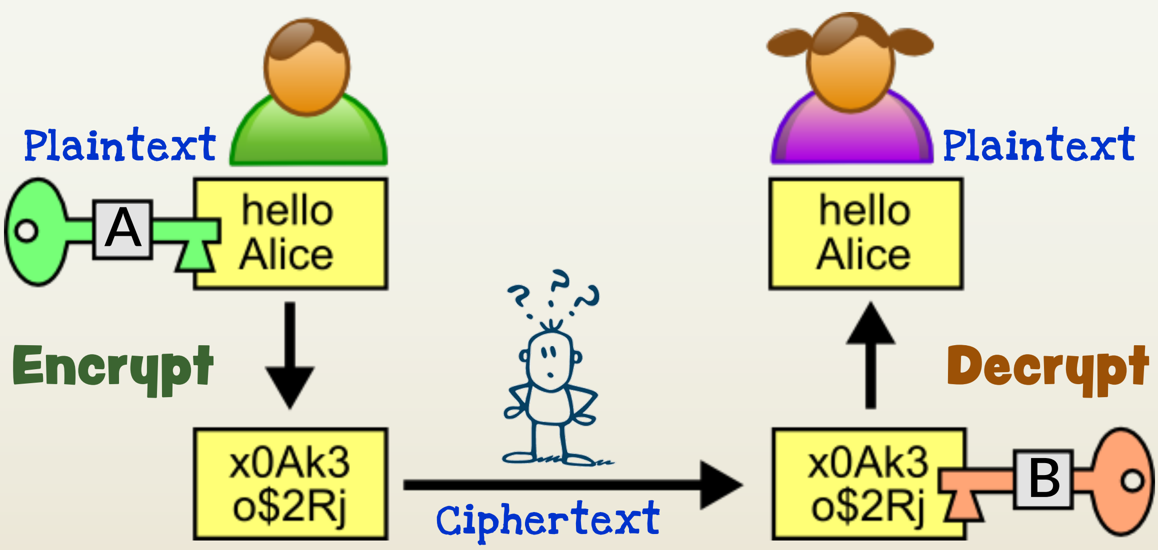
https://www.youtube.com/watch?v=Kf9KjCKmDcU https://www.youtube.com/watch?v=sMOZf4GN3oc

https://www.electronicdesign.com/technologies/embedded-revolution/article/21132412/maxim-integrated-cryptographic-implementations-hardware-vs-software

In plaintext, an intruder can always read your secret conversation



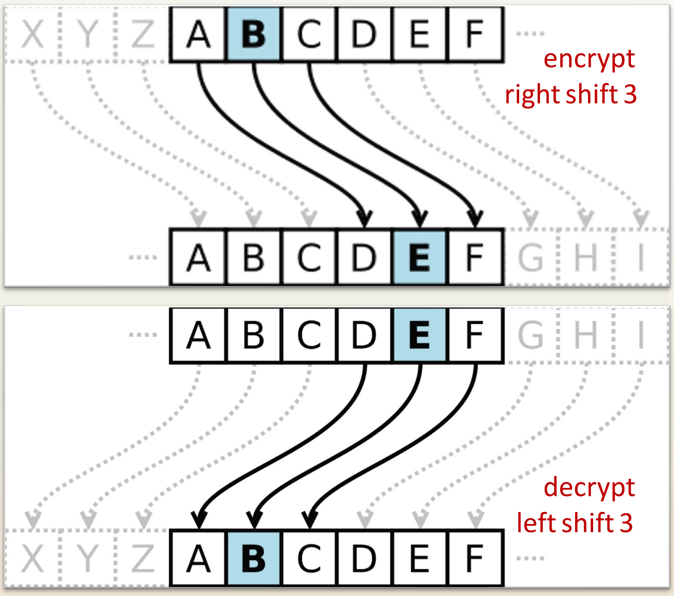
An intruder may catch your encrypted message but not able to read it



Caesar Cipher, also called Caesar shift or **shift cipher**

Caesar cipher hides (***encrypts***) a message by moving each letter a certain number (***a shifted key***) of places to the right along the sorted list of alphabets A-Z

Each letter in the original plaintext is replaced with a different letter that is **a fixed right-shift** of the alphabets A–Z



https://www.youtube.com/watch?v=BdI2whtMyzU

WORKED EXAMPLES

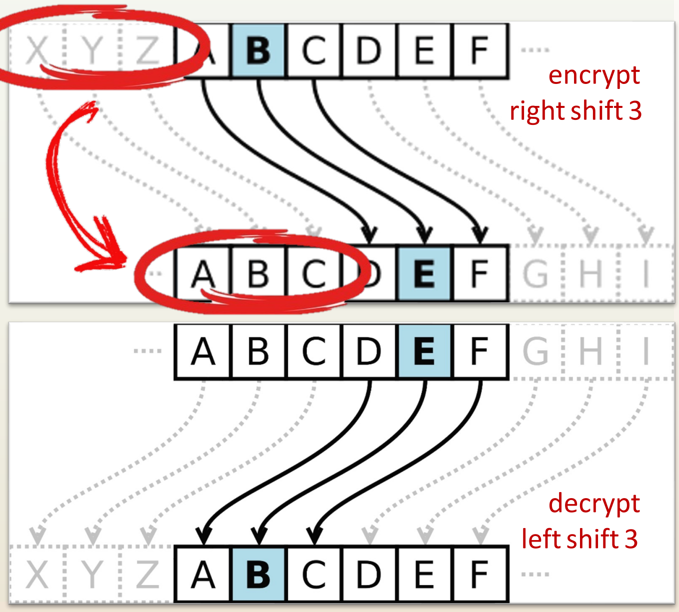
Using Caesar Cipher with key=7, encrypt the word **FOX**

Using Caesar Cipher with key=7, decrypt the word **THW**

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The role of modular arithmetic in Caesar Cipher

When shifted, an alphabet **wraps around** to the first letter A upon reaching the last letter Z



ENCRYPT: $e_k(x) = (x + k) \bmod 26$

DECRYPT: $d_k(x) = (x - k) \bmod 26$

A right rotation of 3 places is equivalent to a left shift of 23

https://www.secplicity.org/2017/05/25/historical-cryptography-ciphers/

Caesar Cipher

Map 26 letters of English alphabet to numbers: A=0, B=1, …, Z=25

Sender: encrypt each letter x in a message: $e_k(x) = (x + k) \bmod 26$

Receiver: decrypt each letter x in a message: $d_k(x) = (x - k) \bmod 26$

key=18 M A T H

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

PRACTICE PROBLEMS

With key=13, encrypt a message: **TREATY IMPOSSIBLE**

With key=4, decrypt a message: **GSQTYXIV WGMIRGI**

PRACTICE PROBLEMS

With key=444, encrypt a message: **GREGORIAN CALENDARS**

The ciphertext "**KBKXEUTK**" is the result of encrypting the word "**EVERYONE**" using Caesar Cipher with the key equals to ____

PRACTICE PROBLEMS

Traditionally, the alphabets in the Caesar Cipher consists of 26 English letters ‘A’ through ‘Z’. In an extended cipher, digits ‘0’ through ‘9’ are included and ordered after the English letters: ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789. In this extended version, perform the following encryption.

Encrypt `IC0S32T` with key `8`

Decrypt `0X22B058` with key `23`

PRACTICE PROBLEMS

Given the characters:
AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz9876543210

Using Caesar Cipher, the plaintext **INSIDEouT4589** is the result of decrypting the word **sx4snoZA2IhGf**, what is the key, k, used for encryption? Give your answer, k, such that k is the least possible key that is more than 1000.