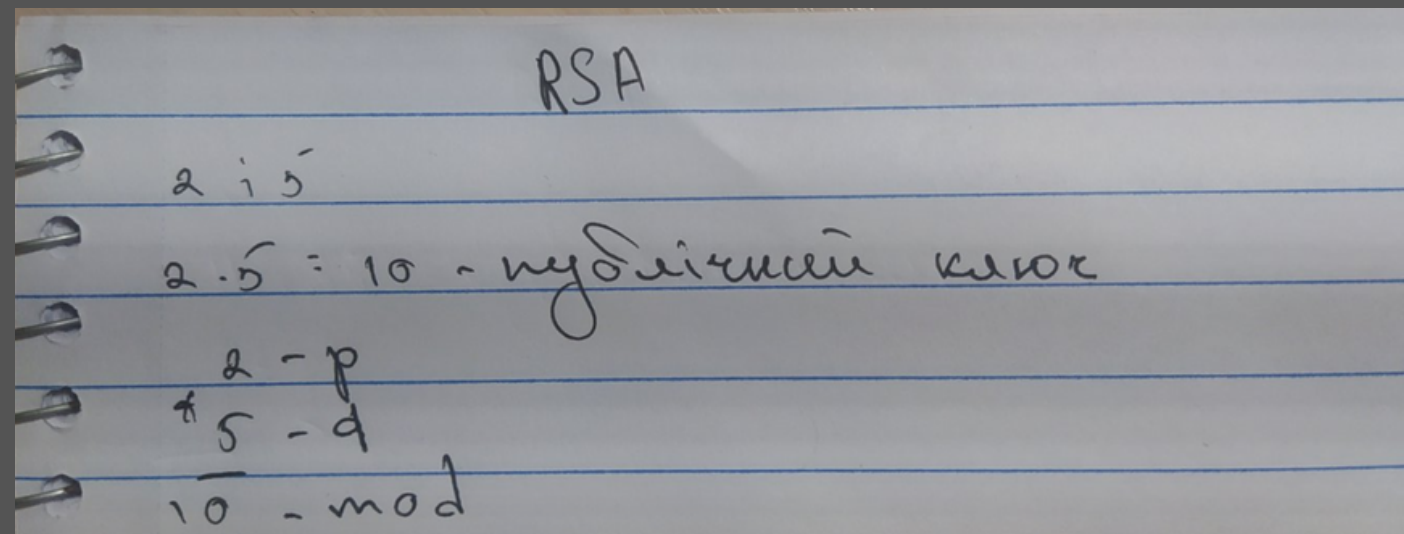




# Качанівський Артем

**Презентація на тему : шифр RSA**

Для початку потрібно  
знайти публічний ключ



Потім потрібно  
перевірити все за  
допомогою формули  
функції Ейлера і ми  
зможемо утворити  
відкритий ключ

$$\phi = (p-1)(q-1)$$
$$\phi = (2-1)(5-1) = 4$$
$$\{e, mod\} = (3, 10)$$

# Далі ми робимо приватний ключ

Приватний ключ -  $(d, e) \cdot 1. \text{ep} = 1; d = 12$   
↓  
 $(d, \text{mod}) = (12, 10)$  12 разів!  
 $12 \cdot 3 = 51$ ; у нас 51, ч зуперим  
 $12 \cdot 3 - 4 \cdot 12 = 51 - 48 = 3$   
 $(12 \cdot 3) - 1 \cdot 4 = 3$



# Далі виконуємо шифрування

Шифрування

Відкрита ключ  $\rightarrow \{3, 10\}$

A	P	T	E	M
1	21	23	5	15

  
$$A = 1^3 \cdot 10 = 0$$
$$P = 21^3 \cdot 10 = 1$$
$$T = 23^3 \cdot 10 = 2$$
$$E = 5^3 \cdot 10 = 3$$
$$M = 15^3 \cdot 10 = 3$$
$$D = 0, 1, 2, 3, 3$$

# Ось кінцевий результат. Дякую за увагу

RSA

$2 \cdot 5$   
 $2 \cdot 5 = 10$  - публічний ключ  
 $2 - p$   
 $5 - q$   
 $10 - mod$

$ep = (p-1)(q-1)$   
 $ep = (2-1)(5-1) = 4$   
 $\{e, mod\} = \{3, 10\}$

Знайдемо  $d$  - приватний ключ -  $(d \cdot e) \% ep = 1$ ;  $d = 13$   
 $\downarrow$   
 $13 \cdot 3 = 39$ ;  $9$  залишок  $39$ ,  $4$  збільшити  
 $(d, mod) = (13, 10)$  13 парів  
 $13 \cdot 3 = 4 \cdot 12 = 39 - 48 = 3$   
 $(13 \cdot 3) \% 4 = 3$

Шифрування  
Відкритий ключ  $\rightarrow \{3, 10\}$

A	P	T	E	M
1	21	23	5	15

$A = 1^3 \% 10 = 0$   
 $P = 21^3 \% 10 = 1$   
 $T = 23^3 \% 10 = 7$   
 $E = 5^3 \% 10 = 5$   
 $M = 15^3 \% 10 = 5$

$D = 0, 1, 2, 3, 5$