



Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій

Лабораторна робота №5

**Безпека інформаційних систем**

«Дослідження криптосистеми Ель-Гамаль»

Виконала:

студентка групи IA-34

Мартинюк Т.В.

Перевірила:

Шимкович Л. Л.

Київ – 2025

**Тема:** Дослідження криптосистеми Ель-Гамаль.

**Хід роботи:**

**Теоретична частина:**

Етап Результати роботи з програмою — X

### Результати тестування

Правильних	10 (100 %)
Неправильних	0 (0 %)
Оцінка тестування	<b>5</b>

  

### Результати шифрування/дешифрування

Шифрування	Пройдено у демонстраційному режимі
Дешифрування	Пройдено у демонстраційному режимі

Далі

**Практична частина:**

Формування ключів:

Обираємо числа P – просте число, та A – первісний елемент для P.

Введення вихідних даних — X

149	10
Табличні значення P і A	Генерувати P і A автоматично
Скасування	Допомога
Далі	

Обираємо закритий ключ Х та обчислюємо публічний ключ В за формулою.

$$Bv = 10^{112} \bmod 149 = 142$$

The image shows two side-by-side calculators for the Diffie-Hellman protocol:

- Calculator 1 (Left):** A yellow header "Діффі - Хеллман". It asks to enter or generate a public key  $X_u$  (1 <  $X_u$  < P-1). The input field contains "112". A button "Згенерувати закритий ключ  $X_v$  автоматично" is present. Below it, it says "Obчисліть ВІДКРИТИЙ КЛЮЧ Ви самостійно або натисніть "Обчислити відкритий ключ Ви автоматично"" and shows the result  $B_v = A^{X_u} \bmod P$  as "142". A button "Обчислити відкритий ключ Ви автоматично" is next to it. Other buttons include "? Допомога" and "Передати відкритий ключ Ви користувачеві V".
- Calculator 2 (Right):** A yellow header "Діффі - Хеллман". It asks for the generation of a private key  $X_v$  (1 <  $X_v$  < P-1). An input field shows "\*\*\*". Below it, it says "Обчислення ВІДКРИТОГО КЛЮЧА Ви  $B_v = A^{X_v} \bmod P$ ". A button "Bv: \*\*\*" is shown. The calculators are connected by a green arrow pointing from the left to the right.

### Шифрування:

Обираємо допоміжне число Y в межах від 1 до p-1. Обчислюємо число E, яке потім буде передано разом з криптограмою. Обчислюємо значення K, що безпосередньо використовується у формуванні криптограми.

$$E_u = A^Y_u \bmod P = 10^{73} \bmod 149 = 134$$

$$K_u = B_v^Y_u \bmod P = 17^{73} \bmod 149 = 114$$

The image shows two side-by-side calculators for the El-Gamal encryption scheme:

- Calculator 1 (Left):** A grey header "Ель-Гамаль - шифрування". It asks to enter or generate a number  $Y_u$  (1 <  $Y_u$  < P-1). The input field contains "73". A button "Згенерувати  $Y_u$  автоматично" is present. Below it, it says "Обчисліть  $E_u$  самостійно або натисніть "Обчислити  $E_u$  автоматично"" and shows the result  $E_u = A^{Y_u} \bmod P$  as "134". A button "Обчислити  $E_u$  автоматично" is next to it. Other buttons include "? Допомога" and "Далі".
- Calculator 2 (Right):** A grey header "Ель-Гамаль - шифрування". It asks for the generation of a number  $Y_v$  (1 <  $Y_v$  < P-1). An input field shows "\*\*\*". Below it, it says "Обчислення числа  $E_v$   $E_v = A^{Y_v} \bmod P$ ". A button "E\_v: \*\*\*" is shown. Below it, it says "Обчислення числа  $K_v$   $K_v = B_u^{Y_v} \bmod P$ ". A button "K\_v: \*\*\*" is shown. At the bottom, it says "Вихідне повідомлення для передачі користувачеві U:" followed by a field containing "\*\*\*\*\*".

Вводимо текст повідомлення та переписуємо його у числовому представленні.

Введіть вихідне повідомлення для надсилання користувачеві V. Для складання повідомлення використовуйте символи із

**перемога**

Числове подання повідомлення:  
Для того, щоб перекласти буквене уявлення повідомлення в цифровий вигляд скористайтесь алфавітом.

$m_{1u}$ :

п	е	р	е	м	о	г	а		
16	6	17	6	13	15	4	1		

Перекласти вихідне повідомлення в числовий вигляд автоматично

Далі

↓



Використовуємо переписане числове представлення повідомлення та раніше обраховане значення K, обчислюємо текст криптограми. На початок вписуємо раніше обраховане значення E та відправляємо одержувачу.

$C1u = m1u \cdot Ku =$	1824
$C2u = m2u \cdot Ku =$	684
$C3u = m3u \cdot Ku =$	1938
$C4u = m4u \cdot Ku =$	684
$C5u = m5u \cdot Ku =$	1482
$C6u = m6u \cdot Ku =$	1710
$C7u = m7u \cdot Ku =$	456
$C8u = m8u \cdot Ku =$	114

Складання криптограми	
Обчислення значень Ci	v
$c_{iv} = m_{iv} \cdot Kv,$	{ i=1..n }
$c1v = m1v \cdot Kv =$	*
$c2v = m2v \cdot Kv =$	*
$c3v = m3v \cdot Kv =$	*
$c4v = m4v \cdot Kv =$	*
$c5v = m5v \cdot Kv =$	*
$c6v = m6v \cdot Kv =$	**
$c7v = m7v \cdot Kv =$	*

На початок складеної криптограми додаємо число Еу і можемо передавати її користувачеві V:

Еу	134
C1	1824
C2	684
C3	1938
C4	684
C5	1482
C6	1710
C7	456
C8	114

Передати складену  
криптограму  
користувачеві V



На початок складеної криптограми додаємо число Еу:

Еу	91
c1	361
c2	114
c3	228
c4	114
c5	399
c6	285
c7	266

--> Повідомлення адресата U адресату V:

**134 1824 684 1938 684 1482 1710 451**

Повідомлення адресата V адресату U:

**91 361 114 228 114 399 285 266**

## Дешифрування:

Використовуючи отримане значення Е (перше число криптограми) обчислюємо значення K.

**Ель-Гамаль-дешифрування**

Розшифровка криптограми користувача V

Отримана криптограма від адресата V, що складається з числа Еу (перше число криптограми) і зашифрованого повідомлення (починаючи з другого числа) - числа с1v...сnv, виглядає так :

**91 361 114 228 114 399 285 266**

Обчисліть Kv самостійно або натисніть кнопку "Обчислити Kv"

$Kv = Ev^{Xu} \bmod P$

Kv :       Обчислити Kv автоматично

$Ev = 91$        $Xu = 112$

**142**      **17**

Середовище передачі даних

P = **149**      A = **10**

Відкритий ключ Ви користувача U: **142**      Відкритий ключ Ву користувача V: **17**

--> Повідомлення адресата U адресату V:

**134 1824 684 1938 684 1482 1710 451**

Повідомлення адресата V адресату U:

**91 361 114 228 114 399 285 266**

Використовуючи знайдене значення K розшифровуємо отриману криптограму.

Переписуємо числове представлення повідомлення у звичайне.

Розшифруйте криптограму самостійно або натисніть кнопку "Розшифрувати криптограму"

 $m_{iv} = c_{iv} / Ku$ 

$m1v = c1v / Kv =$	19
$m2v = c2v / Kv =$	6
$m3v = c3v / Kv =$	12
$m4v = c4v / Kv =$	6
$m5v = c5v / Kv =$	21
$m6v = c6v / Kv =$	15
$m7v = c7v / Kv =$	14

Розшифрувати криптограму автоматично

Далі

Переклад розшифрування криптограми з числового виду в літерний. Для перекладу скористайтесь алфавітом

m1	m2	m3	m4	m5	m6	m7		
т	е	л	е	ф	о	н		

Перевести в літерний вигляд автоматично

РЕЗУЛЬТАТ

→

Переглянути Алфавіт

Середовище передачі даних

$P = 149$        $A = 10$

Відкритий ключ Ви користувача U: 142      Відкритий ключ Ви користувача V: 17

...> Повідомлення адресата U адресату : 134 1824 684 1938 684 1482 1710 451  
Повідомлення адресата V адресату U: 91 361 114 228 114 399 285 266

**телефон**

**перемога**

Вихід

### Ель-Гамаль - дешифрування

Розшифровка криптограми користувача U

Отримана криптограма від адресата U :

134 1824 684 1938 684 1482 1710 456 1

Обчислення числа Ku

$Ku = Eu^{Xv} \bmod P$

$Ku: 114$        $Eu = 134$   
 $Xv = 4$

Розшифрування одержаної криптограми

$m_u = c_{iu} / Ku$

$m1u = c1u / Ku =$	16
$m2u = c2u / Ku =$	6
$m3u = c3u / Ku =$	17
$m4u = c4u / Ku =$	6
$m5u = c5u / Ku =$	13
$m6u = c6u / Ku =$	15
$m7u = c7u / Ku =$	4
$m8u = c8u / Ku =$	1

Переклад розшифрованої криптограми з числового вигляду до буквенного :

m1	m2	m3	m4	m5	m6	m7	m8	
п	е	р	е	м	о	г	а	

← Результати роботи з програмою

## Результати тестування

Правильних	10 (100 %)
Неправильних	0 (0 %)
Оцінка тестування	5

---

## Результати шифрування/дешифрування

Шифрування ПРОЙДЕНО

Дешифрування ПРОЙДЕНО

Далі

**Висновок:** Під час виконання даної лабораторної роботи ми дослідили криптосистему Ель-Гамаль, навчилися шифрувати дешифрувати дані.