



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 ІА-34

Мартинюк Т.В.

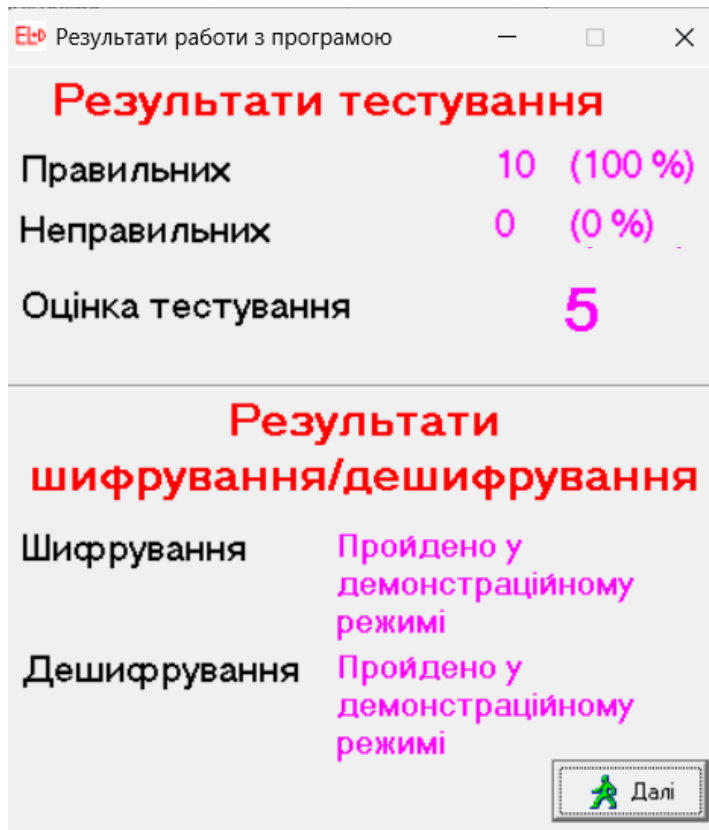
Перевірила:

Шимкович Л. Л.

Тема: Дослідження криптосистеми Ель-Гамаль.

Хід роботи:

Теоретична частина:



Практична частина:

Формування ключів:

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



Обираємо закритий ключ X та обчислюємо публічний ключ B за формулою.

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

Діффі - Хеллман

Формування ключів користувача U

Введіть або згенеруйте ЗАКРИТИЙ КЛЮЧ X_u ($1 < X_u \leq P-1$):

X_u :

Згенерувати закритий ключ X_u автоматично

Обчисліть ВІДКРИТИЙ КЛЮЧ B_u самостійно або натисніть "Обчислити відкритий ключ B_u автоматично"

$B_u = A^{X_u} \bmod P$

B_u :

Обчислити відкритий ключ B_u автоматично

? Допомога

Передати відкритий ключ B_u користувачеві V

Діффі - Хеллман

Формування ключів користувача V

Генерація ЗАКРИТОГО КЛЮЧА X_v

X_v ($1 < X_v \leq P-1$):

X_v :

Обчислення ВІДКРИТОГО КЛЮЧА B_v

$B_v = A^{X_v} \bmod P$

B_v :

Середовище передачі даних

$P =$ $A =$

Відкритий ключ B_u адресата U:

Відкритий ключ B_v адресата V:

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.

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

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

Ель-Гамаль - шифрування

Введення та шифрування повідомлення адресата

Введіть або згенеруйте число Y_u ($1 < Y_u \leq P-1$):

Y_u :

Згенерувати Y_u автоматично

Обчисліть E_u самостійно або натисніть "Обчислити E_u автоматично"

$E_u = A^{Y_u} \bmod P$

E_u :

Обчислити E_u автоматично

Обчисліть K_u самостійно або натисніть "Обчислити K_u автоматично"

$K_u = B_v^{Y_u} \bmod P$

K_u :

Обчислити K_u автоматично

? Допомога

Далі

Ель-Гамаль - шифрування

Введення та шифрування повідомлення адресата

Генерація числа Y_v ($1 < Y_v \leq P-1$):

Y_v :

Обчислення числа E_v

$E_v = A^{Y_v} \bmod P$

E_v :

Обчислення числа K_v

$K_v = B_u^{Y_v} \bmod P$

K_v :

Вихідне повідомлення для передачі користувачеві U:

Числове подання повідомлення:

m_v :

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_{i_u} :

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



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	26	27	28	29	30	31	32
а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я

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

$C1_u = m1_u * K_u =$	1824
$C2_u = m2_u * K_u =$	684
$C3_u = m3_u * K_u =$	1938
$C4_u = m4_u * K_u =$	684
$C5_u = m5_u * K_u =$	1482
$C6_u = m6_u * K_u =$	1710
$C7_u = m7_u * K_u =$	456
$C8_u = m8_u * K_u =$	114

Складання криптограми	
Обчислення значень C_{i_v}	
$c_{i_v} = m_{i_v} * K_v, \quad \{i=1..n\}$	
$c1_v = m1_v * K_v =$	*
$c2_v = m2_v * K_v =$	*
$c3_v = m3_v * K_v =$	*
$c4_v = m4_v * K_v =$	*
$c5_v = m5_v * K_v =$	*
$c6_v = m6_v * K_v =$	**
$c7_v = m7_v * K_v =$	*

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

E_u	134
C_1	1824
C_2	684
C_3	1938
C_4	684
C_5	1482
C_6	1710
C_7	456
C_8	114

Передати складену криптограму користувачеві V

На початок складеної криптограми додаємо число E_v :

E_v	91
c_1	361
c_2	114
c_3	228
c_4	114
c_5	399
c_6	285
c_7	266

---> Повідомлення адресата U адресату V :

134 1824 684 1938 684 1482 1710 456

Повідомлення адресата V адресату U :

91 361 114 228 114 399 285 266

Дешифрування:

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

Ель-Гамаль-дешифрування

Розшифровка криптограми користувача V

Отримана криптограма від адресата V , що складається з числа E_v (перше число криптограми) і зашифрованого повідомлення (починаючи з другого числа) - числа $c_1 v \dots c_n v$, виглядає так:

91 361 114 228 114 399 285 266

Обчисліть K_v самостійно або натисніть кнопку "Обчислити K_v "

$$K_v = E_v^{X_u} \bmod P$$

K_v :

$E_v = 91$
 $X_u = 112$

Обчислити K_v автоматично

Далі

Середовище передачі даних

$P =$ $A =$

Відкритий ключ B_u користувача U :

Відкритий ключ B_v користувача V :

---> Повідомлення адресата U адресату V :

134 1824 684 1938 684 1482 1710 456

Повідомлення адресата V адресату U :

91 361 114 228 114 399 285 266

Використовуючи знайдене значення K розшифровуємо отриману криптограму. Перепишемо числове представлення повідомлення у звичайне.

Розшифруйте криптограму самостійно або натисніть кнопку "Розшифрувати криптограму"

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

? Допомога

$m1v = c1v / K_v =$	19
$m2v = c2v / K_v =$	6
$m3v = c3v / K_v =$	12
$m4v = c4v / K_v =$	6
$m5v = c5v / K_v =$	21
$m6v = c6v / K_v =$	15
$m7v = c7v / K_v =$	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 V_u користувача U: 142

Відкритий ключ V_v 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

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 K_u

$K_u = E_u^{X_v} \bmod P$

$E_u = 134$
 $X_v = 4$
 $K_u = 114$

Розшифрування одержаної криптограми

$m_{iu} = c_{iu} / K_u$

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

Переклад розшифрованої криптограми з числового вигляду до буквеного:

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, навчились шифрувати дешифрувати дані.