# ЛАБОРАТОРНА РОБОТА № 5-6

# КРИПТОГРАФІЯ З ВІДКРИТИМ КЛЮЧЕМ . ФУНКЦІЯ ҐЕШУВАННЯ

**Мета роботи:** ознайомитися з найпростішою функцією ґешування та схемами електронного цифрового підпису RSA та ElGamal.

**Використовуване програмне забезпечення:** пакети математичних обчислень MathCad і середа розробки GNU Octave.

## Теоретичні відомості

* + 1. **Асиметричні криптосистеми**

Ефективними системами криптографічного захисту даних є *асиметричні криптосистеми*. В таких системах для зашифрування даних використовується один ключ, а для розшифрування – інший. Причому ключі пов’язані між собою певним математичним співвідношенням, що робить можливим процес адекватного розшифрування. Концепція таких криптосистем основана на застосуванні однонаправлених функцій з секретом, що дозволяє легко отримати відкритий ключ із секретного, але не навпаки.

Двухключова криптографія використовується в двух схемах: *цифрового підпису* і *спрямованого шифрування*. В першому випадку повідомлення підписується закритим ключем і будь-яка особа може упевнитися в його дійсності за допомогою відкритого ключа. В схемі спрямованого шифрування, навпаки, повідомлення зашифровується на відкритому ключі отримувача. Розшифрувати повідомлення має можливість тільки сам отримувач за допомогою свого секретного ключа.

В протоколах цифрового підпису застосовується так звана «ґеш- функція».

*Ґеш-функціей* називається перетворення *H*, що переводить повідомлення M довільної довжини у повідомлення *H(M)* фіксованої довжини. Ґеш-функція повинна задовольняти таким вимогам:

* + не вище чим поліноміальна складність обчислення значення ґеш-функції;
	+ не нижче чим експоненціальна складність визначення повідомлення *Mi* по відомому значенню *H(Mi)*;
	+ практична захищеність від колізій, коли можна знайти *Mi* та *Mj*, такі, що *H(Mi)*=*H(Mj)*, з імовірністю не вище чим *Pk*, де *Pk* завідомо задане значення.
		1. **Алгоритм RSA в схемі спрямованого шифрування**

Алгоритм RSA запропонували у 1978 р. три автора Р.Райвест, А.Шамір, А.Адлеман. Стійкість алгоритму базується на складності факторизації великих чисел і трудності обчислення дискретних логарифмів.

Алгоритм RSA використовується в моделі взаємної недовіри. Її сутність полягає в тім, що кожен користувач генерує ключі сам собі. Особистий ключ залишає в себе і забезпечує його строгу конфіденційність. Відкритий ключ розсилає всім користувачам, з якими він зв'язаний. Він також забезпечує цілісність і дійсність відкритих ключів. Таким чином, будь-хто може надіслати йому повідомлення, зашифроване на відомому відкритому ключі, яке може прочитати тільки сам користувач, бо тільки він володіє відповідним секретним ключем.

**Алгоритм 3.1**

* 1. Обираємо модуль перетворень *N=P\*Q*, де *P, Q* – випадкові великі прості числа.
	2. Обчислюємо

(*N*)

(*P* 1)(*Q*

1) , де

(*N*)

- функція Ейлера,

що вказує кількість додатних цілих чисел в інтервалі від 1 до *N*, що взаємно прості з *N*.

* 1. Відкритий ключ *e* вибирається випадково так, щоб виконувались умови

1 *e* (*N*),

*НОД* (*e*,

(*N*)) 1

* 1. Обчислюємо закритий ключ *d* з умови

*ed* 1mod (*N* ), *або*

*d e* 1 mod(*P*

,

1)(*Q* 1)

використовуючи розширений алгоритм Евкліда. Ключ *d* та модуль *N*

повинні бути взаємно простими*.*

* 1. Зашифрування повідомлення M відбувається за формулою

*C Me* mod *N*

* 1. Розшифрування повідомлення відбувається за формулою

*M Cd* mod *N*

* + 1. **Цифровий підпис Эль-Гамаля**

Цифровий підпис Эль-Гамаля базується на великій обчислювальній складності задачі дискретного логарифмування.

Позначення:

*p* – велике просте число, модуль перетворень;

*a* – первісний корінь за модулем *p; x –* секретний ключ;

*y –* відкритий ключ *y ax* mod *p* ;

*M* – повідомлення, що підписується (*M<p*);

*r, s = f(M,x)* – підпис.

**Алгоритм 3.2**

Формування підпису Эль-Гамаля

1. Згенерувати випадкове число *k*, що задовольняє умовам

*0<k<p-1* и *НОД(k,p-1)=1*

1. Обчислити *r=ak(mod p)*
2. Обчислити *s* з рівняння

*M=xr+ks (mod(p-1))*

З теорії чисел відомо, що таке рівняння має рішення для s, якщо

*НОД(k,p-1)=1.*

Перевірка підпису Эль-Гамаля.

Якщо *(aM)=axraks=yrrs (mod p)* підпис є дійсним.

## Завдання на лабораторну роботу

* + 1. Створіть ґеш-образ повідомлення

«ВЫДАТЬ \_ СТО \_ ГРН \_ ГЛБУХ \_ [ФАМИЛИЯ]»,

з використанням формули

H i = ( H i – 1 + M i – 1 ) 2 mod 33 і кодової таблиці. Значення H 0 = 9 .

Таблиця 3.1 – Кодова таблиця

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | 1 | 00001 | И | 9 | 01001 | С | 17 | 10001 | Щ | 25 | 11001 |
| Б | 2 | 00010 | К | 10 | 01010 | Т | 18 | 10010 | Ъ | 26 | 11010 |
| В | 3 | 00011 | Л | 11 | 01011 | У | 19 | 10011 | Ы | 27 | 11011 |
| Г | 4 | 00100 | М | 12 | 01100 | Ф | 20 | 10100 | Ь | 28 | 11100 |
| Д | 5 | 00101 | Н | 13 | 01101 | Х | 21 | 10101 | Э | 29 | 11101 |
| Е | 6 | 00110 | О | 14 | 01110 | Ц | 22 | 10110 | Ю | 30 | 11110 |
| Ж | 7 | 00111 | П | 15 | 01111 | Ч | 23 | 10111 | Я | 31 | 11111 |
| З | 8 | 01000 | Р | 16 | 10000 | Ш | 24 | 11000 | \_ | 32 | 00000 |

Ґ еш-образ повідомлення представте в двійковому вигляді.

* + 1. Використовуючи відкритий *e* = 7 і закритий *d* = 3 ключі та модуль *n* = 33 схемы RSA, зформуйте та перевірте цифровий підпис для повідомлення.

«ВЫДАТЬ \_ СТО \_ ГРН \_ ГЛБУХ \_ [ФАМИЛИЯ]»,

Ґеш-образ візьміть із завдання 3.2.1; цифровий підпис представте в двійковому виді.

Сформуйте та перевірте цифровий підпис зформованого ґеш- образа за допомогою схеми ElGamal.

* + 1. Для заданого повідомлення в двійковому виді,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 00101011 | 10001000 | 11100001 | 10111010 | 00000000 |
| 01101000 | 01000000 | 11000100 | 10101101 | 01101001 |
| 01110011 | 01000000 | 01001000 | 00110100 | 00000101 |
| 01001100 | 00001100 | 10101001 | 00111010 | 00011001 |

- відокремліть повідомлення і цифровий підпис, створений за допомогою алгоритму RSA (5 біт);

* повідомлення і цифровий підпис представте у десятковому виді;
* за допомогою відкритого ключа *e* = 17 і модуля *n* = 33 розшифруйте цифровий підпис;
* сформуйте ґеш-образ відокремленого повідомлення (см. завдання 3.2.1);
* перевірте коректність поставленого підпису, порівнявши результати двох попередніх пунктів;
* прочитайте повідомлення.

## Зміст звіту

* + 1. Титульний лист, тема і мета роботи.
		2. Відповіді на контрольні питання.
		3. Опис алгоритмів RSA та ElGamal.
		4. Тексти програм
		5. Результати розрахунків.

## Контрольні питання

* + 1. Поняття криптографії з відкритим ключем.
		2. Поняття ґеш-функції. Її властивості.
		3. Модель взаємної недовіри.
		4. Загальна схема формування та перевірки цифрового підпису.
		5. Загальна схема спрямованого шифрування.
		6. Схема цифрового підпису RSA.
		7. Доказати математично коректність алгоритму RSA.
		8. Схема цифрового підпису ElGamal.
		9. Доказати математично коректність алгоритму ElGamal. 3.4.10Від чого захищає цифровий підпис? Яким чином?