



Diffi-Hellman key exchange

ElGamal encryption

Розробила: старший викладач кафедри ПМА Бай Ю.П.



Організаційні питання



Властивості асиметричних алгоритмів



Дискретне логарифмування



Обмін ключами за Діффі-Хеллманом



Криптосистема Ель-Гамала

Алгоритми асиметричного шифрування є достатньо затратними за ресурсам і часом. На практиці для шифрування даних використовуються симетричні алгоритми, а розсилка ключів здійснюється з використанням алгоритмів асиметричного шифрування з **відкритим ключем одержувача даних**.

Симетричне шифрування

Передбачає використання
однакових ключів для шифрування і розшифрування

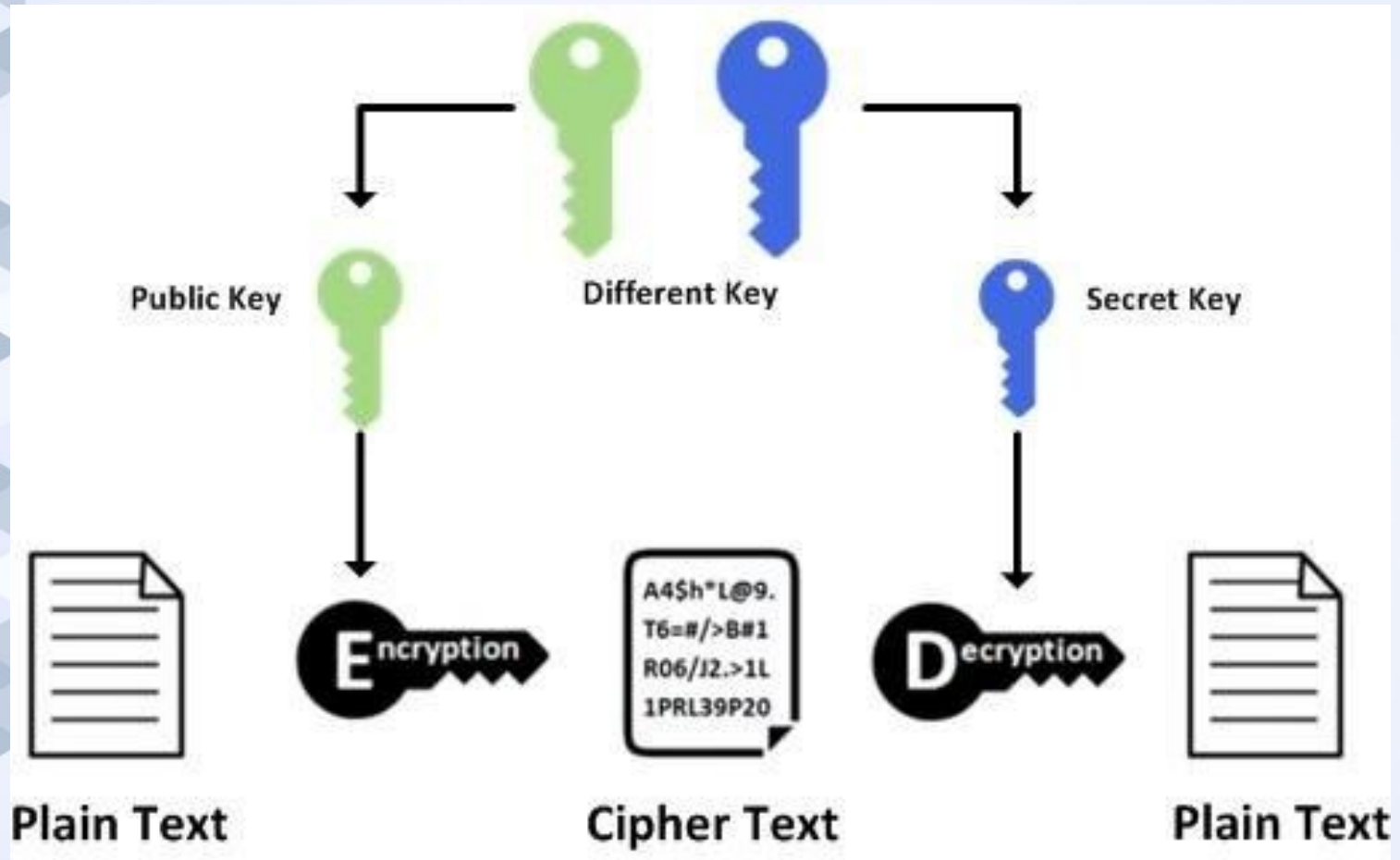
- DES
- Triple-DES
- GOST 28147-89
- Rijndael

Асиметричне шифрування

Алгоритм використовує
різні ключі для шифрування і розшифрування

- RSA
- Diffie-Hellman
- El Gamal
- Elliptic-curve Cryptography

Асиметричне шифрування




Для шифрування і розшифрування використовуються **два різні ключі**

Властивості асиметричних алгоритмів

Ключі: *Public key* – KU
 Private key – KR

- 1) Легко обчислити (KU, KR)
- 2) Легко зашифрувати повідомлення, використовуючи відкритий ключ: $C = E_{KU}(M)$
- 3) Легко розшифрувати повідомлення, використовуючи закритий ключ: $M = D_{KR}(C)$
- 4) Складно, знаючи відкритий ключ, знайти закритий ключ: $KU \nrightarrow KR$
- 5) Складно, знаючи зашифроване повідомлення та відкритий ключ, знайти початкове повідомлення: $(C, KU) \nrightarrow M$



Задача є обчислювально **“легкою”**, якщо її складність пропорційна n^a , де n – довжина входу (n^a – поліном степеня a).

Задача є обчислювально **“складною”**, якщо її складність пропорційна 2^n , де n – довжина входу.

Всі алгоритми з відкритим ключем засновані на використанні так званих **односторонніх функцій**.

Алгоритм Діффі-Хеллмана (1976)



Whitfield Diffie



Martin Hellman

Математичне підґрунтя D-H

В основі алгоритму Діффі-Хеллмана полягає складність задачі **дискретного логарифмування**

$$a^x = b \rightarrow x = \log_a(b)$$

$$a^x \pmod{p} = b \rightarrow x = ?$$

Приклад: $3^4 \pmod{17} = 13$ ($3, 17$ – відкриті, 4 – закрите число)

Нехай дано: $3^x \pmod{17} = 13$. Як знайти x ?

$$3^1 = 3 \quad 3^2 = 9 \quad 3^3 = 10 \quad 3^4 = 13 \quad 3^5 = 5 \quad \dots$$

Назад складно! Маємо **односторонню функцію**:

$$F(x) = g^x \pmod{p}$$

Схема алгоритму Діффі-Хеллмана

$$f(x) = g^x \bmod p$$

	<i>Alice</i>			<i>Bob</i>	
1	Обирає і публікує прості числа g, p (частини відкритого ключа)	{3, 17}			
2	Обирає секретний ключ a	4		Обирає секретний ключ b	6
3	Обчислює і публікує $A = g^a \bmod p$	A=13		Обчислює і публікує $B = g^b \bmod p$	B=15
4	Обчислює $K = B^a \bmod p$	16		Обчислює $K = A^b \bmod p$	16

Доведення рівності ключів

$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$

Шифрування **Ель-Гамала** (1985)

У 1985 році опублікував статтю під назвою «Криптосистема з відкритим ключем і схема цифрового підпису на основі дискретних логарифмів»

В основі алгоритму Ель-Гамала полягає складність задачі **дискретного логарифмування**



Taher El-Gamal

Схема Ель-Гамаля

- **Генерація ключа:** прості числа p , g та ціле число x :
 $g < p-1$, $x < p-1$
- $y = g^x \bmod p$
- $\{g, p, y\}$ – відкритий ключ, $\{x\}$ – закритий ключ

Шифрування

- M – відкритий текст
- k – випадкове число, взаємно просте з $(p-1)$
- $a = g^k \bmod p$, $b = (y^k \cdot M) \bmod p$
- $C = \{a, b\}$ - шифротекст

Розшифрування

$$M = (b \cdot a^{p-1-x}) \bmod p$$