ЛЕКЦІЯ 7

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

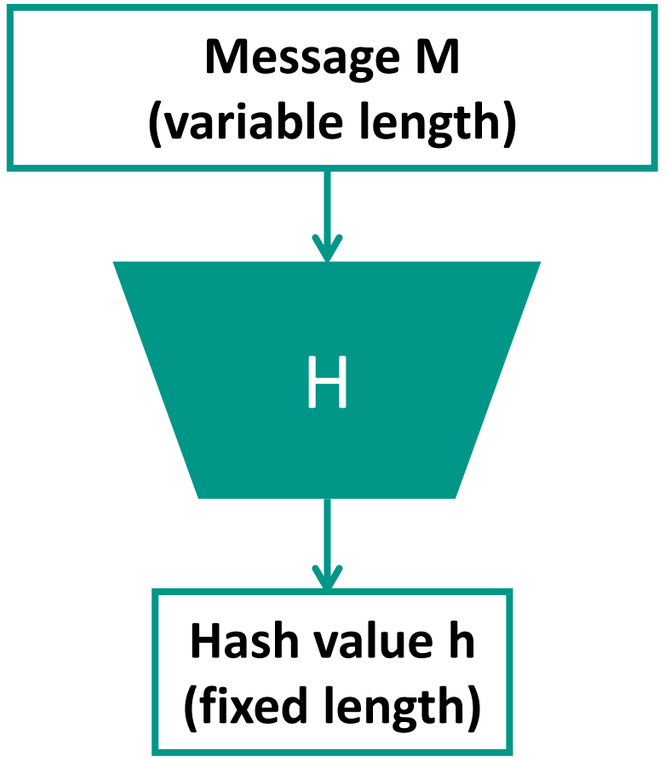
Цифровий підпис

План

1. Криптографічні хеш-функції
2. Процедури створення та перевірки підпису
3. Схеми цифрового підпису RSA та Ель-Гамаля
4. Стандарт цифрового підпису DSS

1. Криптографічні хеш-функції

Хеш-функція являє собою функцію, математичну або іншу, що отримує на вхід рядок змінної довжини і перетворює його в рядок фіксованої, зазвичай меншої, довжини

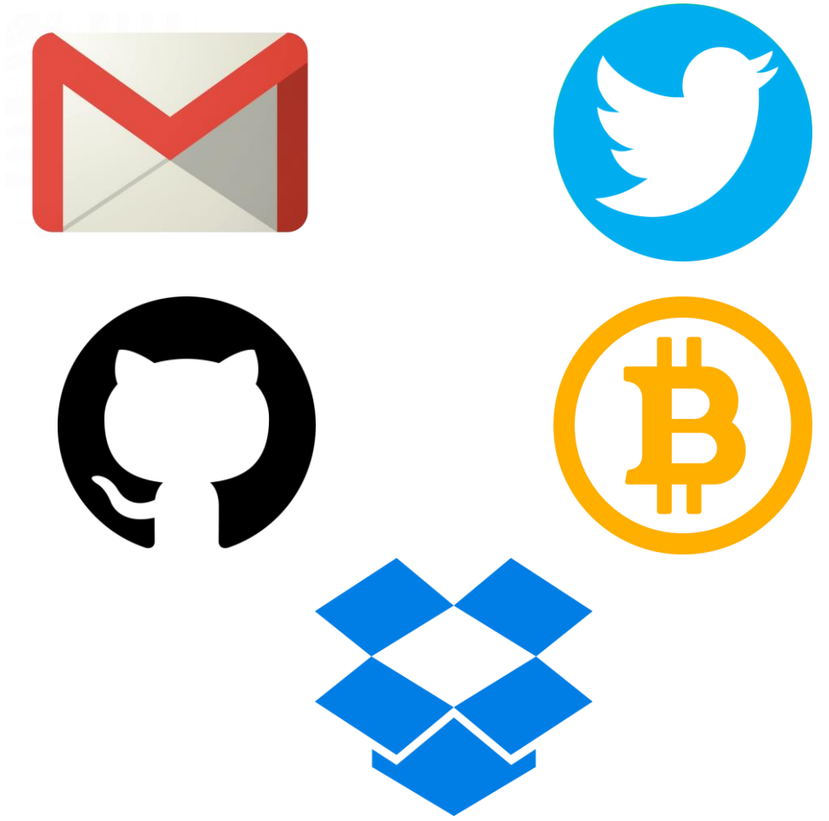


Результат хеш-функції називають хешем, хеш-значенням або дайджестом

1. Криптографічні хеш-функції

Застосування хеш-функції

- ✓ Перевірка цілісності повідомлень та файлів;
- ✓ Генерація і перевірка (електронного) цифрового підпису;
- ✓ Перевірка пароля;
- ✓ Ідентифікатор файлу або даних.



1. Криптографічні хеш-функції

Принцип роботи криптографічної хеш-функцій

Повідомлення *M* має бути представлене у двійковій формі і розбите на окремі блоки M_i довжиною *n* біт кожний

Більшість хеш-функцій мають вигляд:

$$h_i = H(M_i, h_{i-1}),$$ де

M_i – черговий блок повідомлення *M*;

h_{i-1} – хеш-значення усіх попередніх блоків *M* (має довжину також n біт)

1. Криптографічні хеш-функції

Принцип роботи криптографічної хеш-функцій

При обчисленні хеш-значення для першого блоку M_1 використовується деяке початкове хеш-значення h_0, яке можна вибрати випадковим *IV* або фіксованим (наприклад, $h_0 = 0$ – у найпростішому випадку)

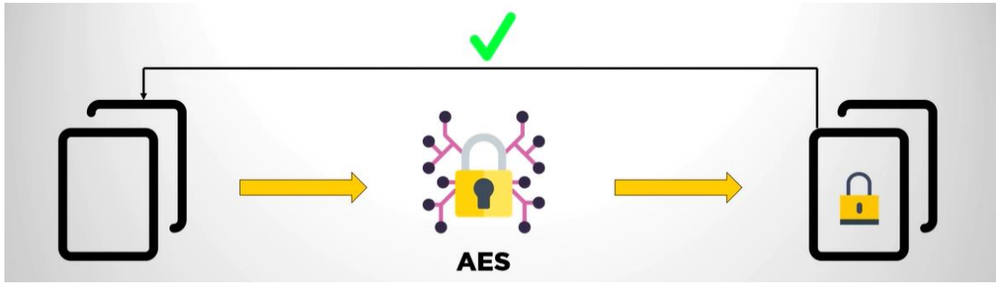
Хеш-значення, обчислене при використанні останнього блоку повідомлення, вважається хеш-значенням усього повідомлення *M*

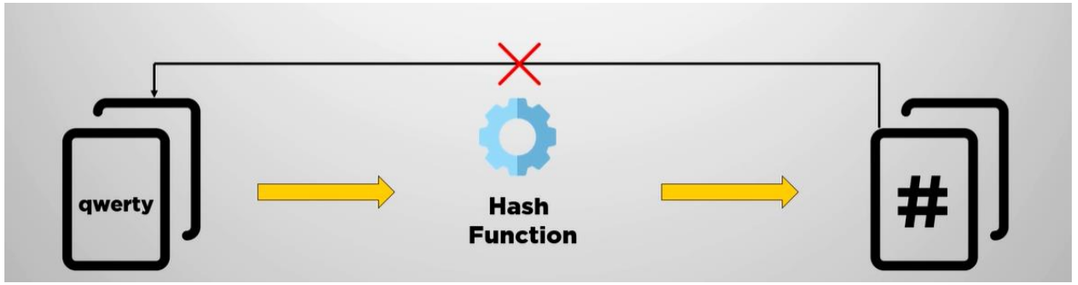
1. Криптографічні хеш-функції

Основні властивості криптографічної хеш-функції

1) Детермінованість – для однакових повідомлень *M* функція має повертати однакові хеш-значення *h*;

2) Односторонність – за значенням *h* неможливо відновити *M*;

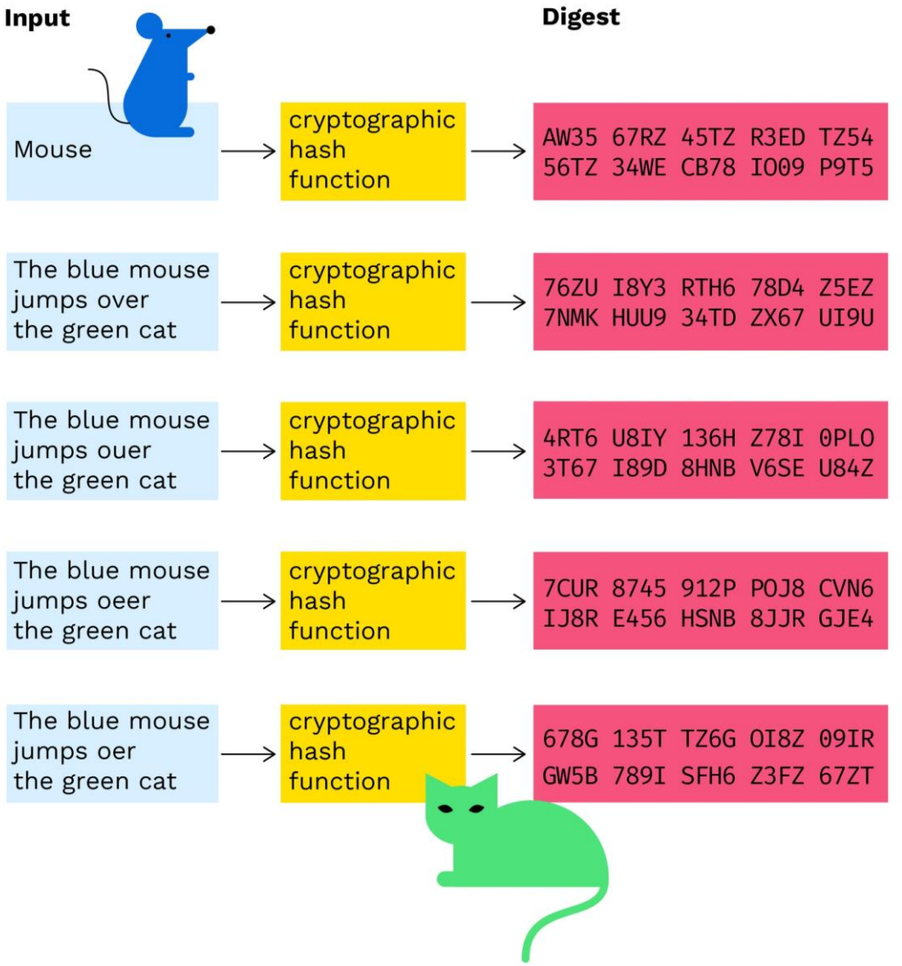




1. Криптографічні хеш-функції

Основні властивості криптографічної хеш-функції

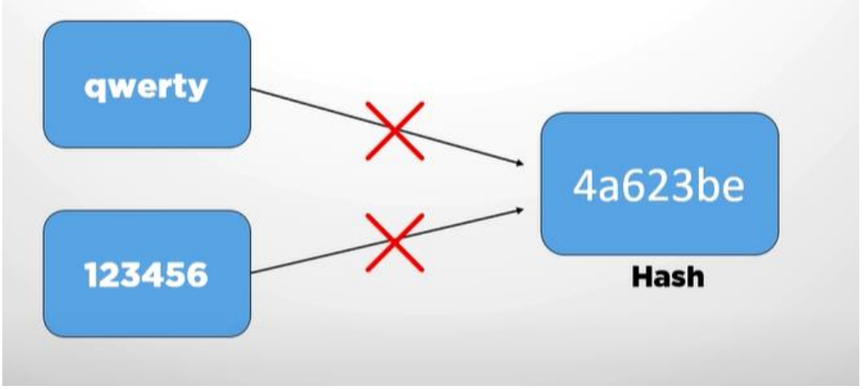
3) Наявність лавинного ефекту – будь-які, навіть незначні, зміни у повідомленні *M* призводять до значних змін у хеш-значенні *h*;



1. Криптографічні хеш-функції

Основні властивості криптографічної хеш-функції

4) Відсутність колізій (унікальність хеша) – ймовірність співпадіння хеш-значень двох різних повідомлень повинна бути надзвичайно малою;



5) Висока швидкість роботи.

1. Криптографічні хеш-функції

Порівняння деяких хеш-функції

Хеш-функція	Рік	Розробники	Довжина блоку	Довжина дайджесту	Кількість раундів
MD5	1992	Ronald Rivest	512	128	64
RIPEMD	1992	The RIPE Consortium	512	128	48
SHA-1	1995	NSA	512	160	80
SHA-256	2002	NSA	512	256	80
SHA-512	2002	NSA	1024	512	80
Whirlpool	2004	Vincent Rijmen, Paulo Barreto	512	512	10
BLAKE-256	2008	Jean-Philippe Aumasson, Luca Henzen, Willi Meier, Raphael C.-W. Phan	512	256	14
Купина	2014	ПАТ «Інститут інформаційних технологій»	512	від 8 до 512 біт	10 або 14

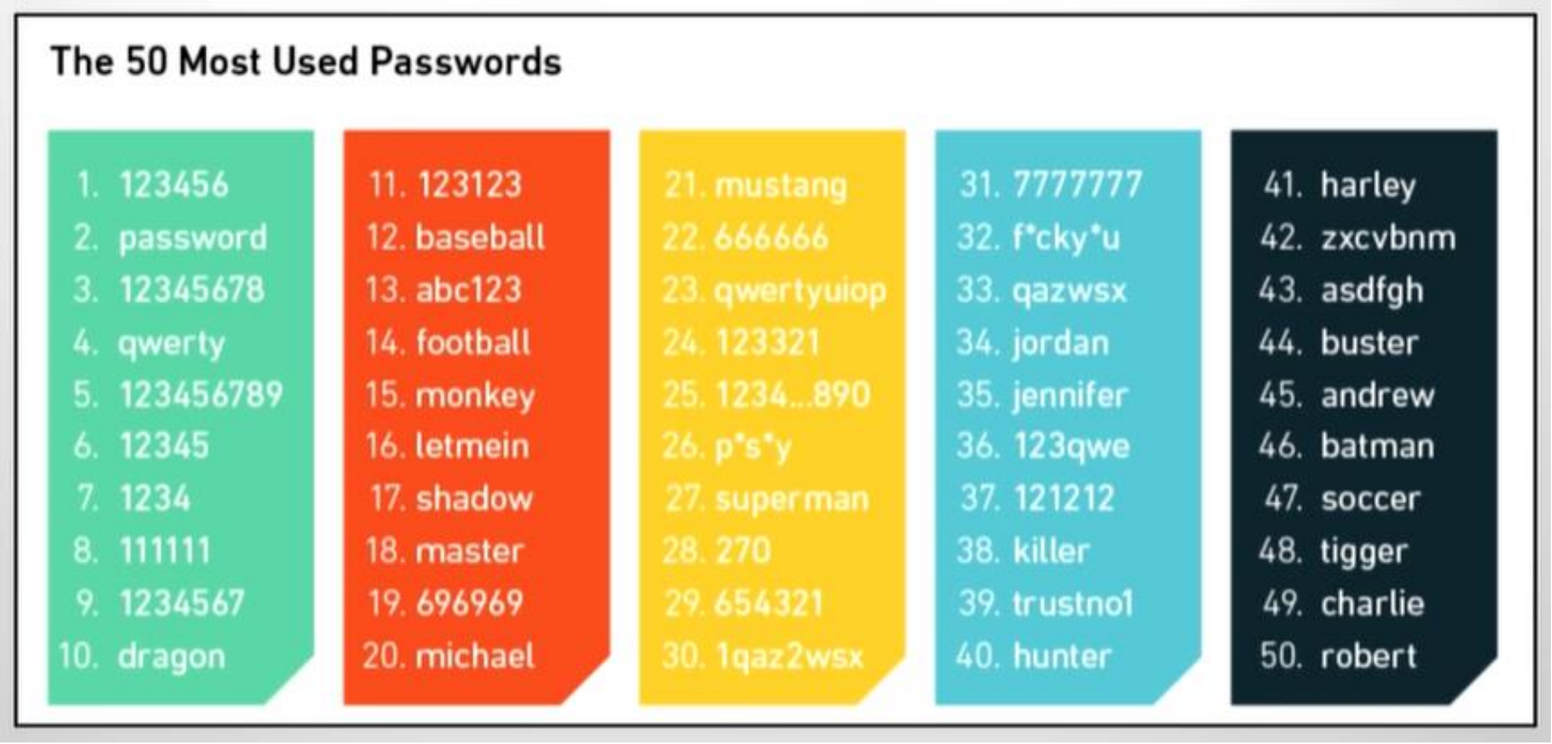
1. Криптографічні хеш-функції

Наприклад, у twitter використовується SHA-256 для збереження паролів користувачів:

Users	Hash
User1	YY9J3lES8K
User2	HTOjXKSLBG
User3	CWBQB3R5G
User4	EGPR20YLY5
User5	CARPNNFIJW
User6	PJLJQDRVCO
User7	CH28YHE5IQ

1. Криптографічні хеш-функції

Обчисливши, хеш-значення найчастіше вживаних паролів, можна підібрати пароль:



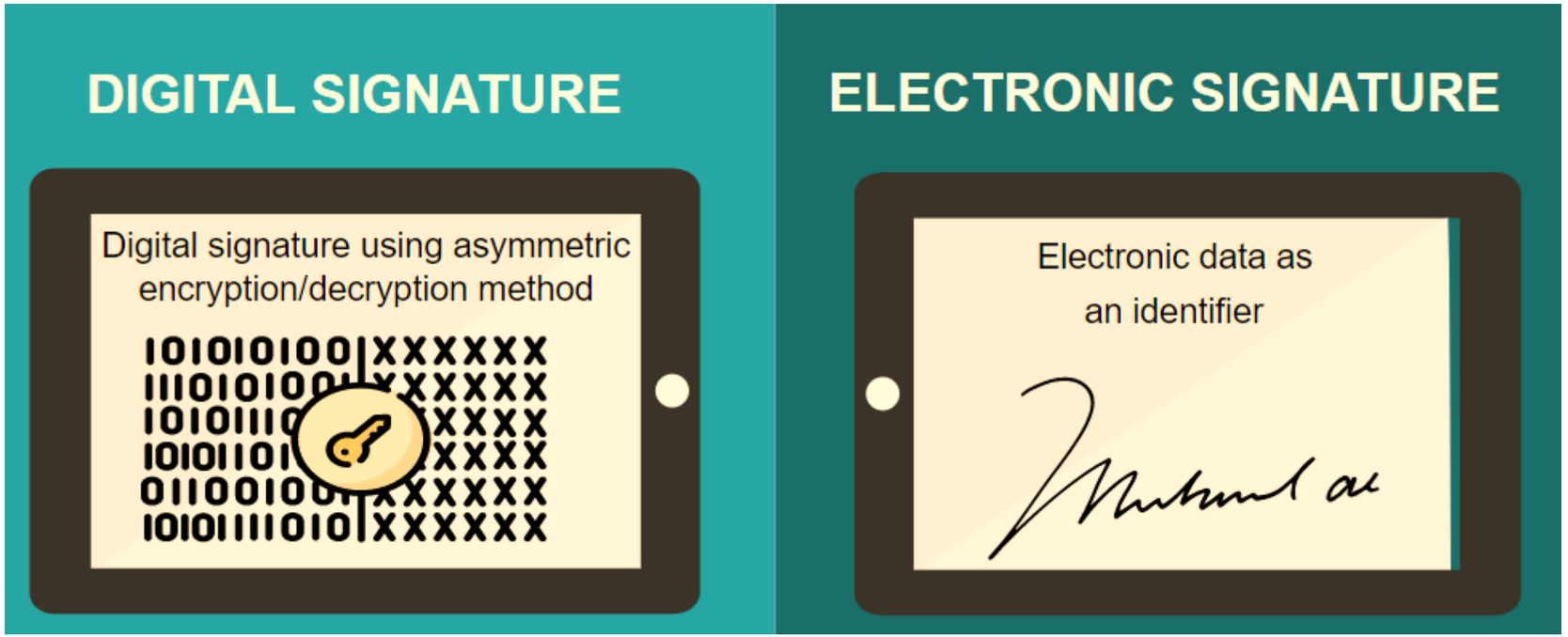
Password	Hash
123456	LRHZAFVUZM
qwerty	R6JTUOGLUG
letmein	YB14YN8280
iloveyou	CARPNNFIJW
654321	4LEJZ8EBB5
mypassword	EAHY7W8LH7
trytohackme	G6GP9LMT99

2. Процедури створення та перевірки підпису

Електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов’язуються і використовуються ним як підпис.

(Електронний) цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.

2. Процедури створення та перевірки підпису



Цифровий підпис є видом електронного підпису і використовує криптографічні хеш-функції і ключі

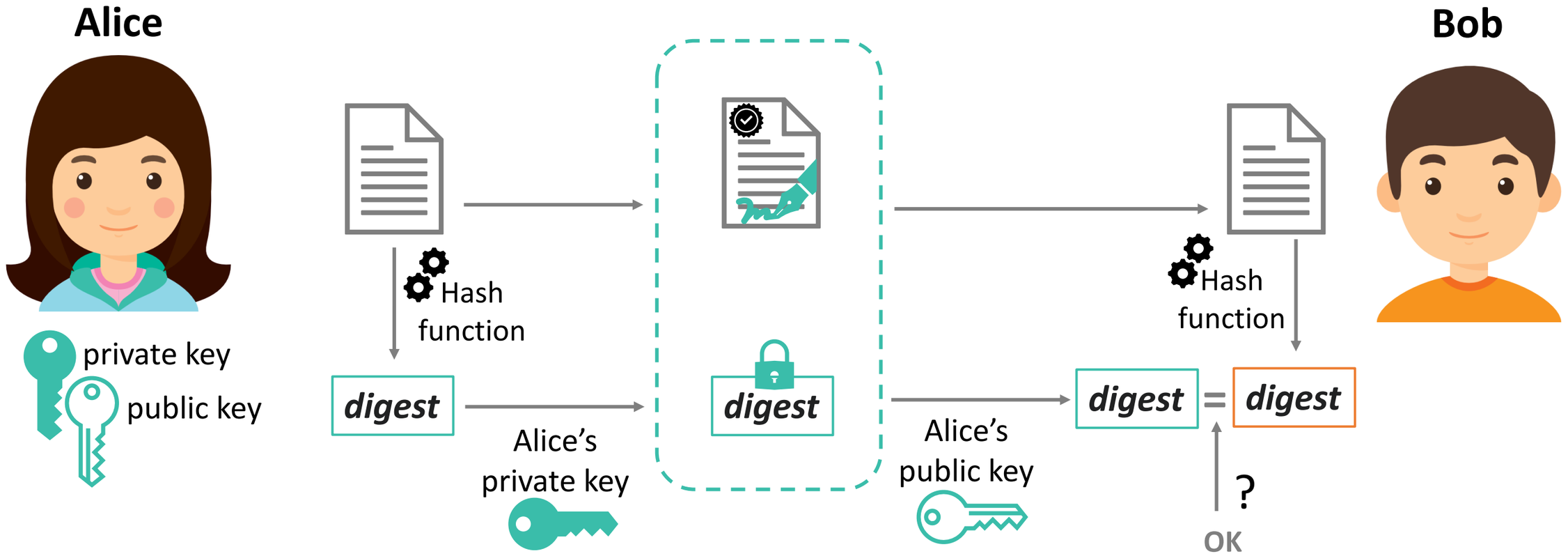
2. Процедури створення та перевірки підпису

1. Генерація пари ключів. За допомогою алгоритму генерації ключів створюється пара ключів – закритий (для створення підпису) та відкритий (для перевірки підпису).

2. Формування підпису. Для заданого електронного документу за допомогою деякої хеш-функції обчислюється хеш-значення, після чого воно зашифровується із використанням закритого ключа підписувача. Зашифрований дайджест і є ЦП для даного документу.

3. Перевірка (верифікація) підпису. Для отриманого документу одержувач знову обчислює його хеш-значення, після чого за допомогою відкритого ключа підписувача дешифрує ЦП. Якщо хеші рівні – підпис справжній.

2. Процедури створення та перевірки підпису



2. Процедури створення та перевірки підпису

Інфраструктура відкритих ключів

- ✓ Центр сертифікації ключів;
- ✓ Центр реєстрації;
- ✓ Каталог (репозітарій, реєстр) сертифікатів;
- ✓ Сервер відновлення ключів;
- ✓ Користувачі (кінцеві суб'єкти);
- ✓ Нормативні документи.

2. Процедури створення та перевірки підпису

Управління ключами

Управлянням ключами займаються центри сертифікації ключів (ЦСК), що забезпечують:

- доступ користувача до справжнього відкритого ключа іншого користувача;
- захист ключів від підміни зловмисником;
- організацію відкликання ключа у випадку його компрометації.

Сертифікат, який видається ЦСК дозволяє підтвердити дані про власника і його відкритий ключ

3. Схеми цифрового підпису RSA та Ель-Гамаля

Схема цифрового підпису RSA

Закритий ключ: (d, n)

Відкритий ключ: (e, n)

Підписування

ЦП для $h(M)$ буде мати вигляд: $s = h(M)^d mod\ n$

Перевірка підпису

Приймається пара (M, s) і обчислюється $h(M)$ і порівнюється з $s^e mod\ n = = (h(M)^d mod\ n)^e\ mod\ n = h(M)$

3. Схеми цифрового підпису RSA та Ель-Гамаля

Приклад 3.1: Підписати та перевірити підпис повідомлення M хеш-значення, якого $h(M) = 88$.

$p = 17, q = 11$

$n = 187, \varphi(n) = 160$

Закритий ключ: $d = 23$

Відкритий ключ:

$e = 7$

Підписування:

$s = h(M)^d mod\ n =$

$= 88^{23} mod\ 187 = 11$

Перевірка підпису

Приймається пара $(M, 11)$ та дешифрується хеш:

$s^e mod\ n = 11^7 mod\ 187 = 88$

3. Схеми цифрового підпису RSA та Ель-Гамаля

Схема цифрового підпису Ель-Гамаля

Закритий ключ: x

Сесійний ключ: k

Відкритий ключ: (p, g, y)

Підписування

ЦП для $h(M)$ буде пара:

$$r = g^k mod\ p$$

$$s = k^{-1}(h(M) - xr) mod\ p - 1$$

Перевірка підпису

Приймається (M, r, s)

і підпис вважається дійсним, якщо:

$$g^{h(M)} \equiv y^r r^s (mod\ p)$$

3. Схеми цифрового підпису RSA та Ель-Гамаля

Приклад 3.2: Підписати та перевірити підпис повідомлення M хеш-значення, якого $h(M) = 14$.

$p = 19, g = 10$

Закритий ключ: $x = 16$

Сесійний ключ: $k = 5$

$y = g^x mod\ p = 10^{16} mod\ 19 = 4$

Відкритий ключ:

$(p, g, y) = 19, 10, 4$

Підписування

$r = 10^5 mod\ 19 = 3$

$s = 5^{-1}(14 - 16 \cdot 3) mod\ 18 =$

$= -374\ mod\ 18 = 4$

$5 \cdot ? \equiv 1\ mod\ 18 \rightarrow 5^{-1} mod\ 18 = 11$

(за розширеним алгоритмом Евкліда)

Перевірка підпису

Приймається $(M, 3, 4)$:

$g^{h(M)} mod\ p = 10^{14} mod\ 19 = 16$

$y^r r^s\ mod\ p\ = 4^3 \cdot 3^4 mod\ 19$

$= 16$

4. Стандарт цифрового підпису DSS

Національний інститут стандартів і технології США (NIST) розробив федеральний стандарт цифрового підпису DSS (Digital Signature Standard)

Для створення цифрового підпису використовується алгоритм DSA (Digital Signature Algorithm)

Як хеш-алгоритм стандарт передбачає використання алгоритму SHA-1 (Secure Hash Algorithm)

4. Стандарт цифрового підпису DSS

Генерація ключів у DSA

1. Генерується просте число p, таке що $2^{L-1} < p < 2^L$, $512 \leq L \leq 1024$ і L кратне 64

2. Обирається q – простий дільник $p - 1$, таке $2^{159} < q < 2^{160}$

3. Обчислюється $g = h^{(p-1)/q} \ mod \ p$, де h будь-яке ціле число таке, що $0 \leq h \leq p - 1$ та $h^{(p-1)/q} \ mod \ p > 1$

6. Вибирається x – випадкове ціле число, таке що $0 < x < q$

5. Обчислюється $y = g^x \bmod p$

6. x і y є закритим і відкритим ключами, відповідно

4. Стандарт цифрового підпису DSS

Підпис повідомлення

Підпис повідомлення M із використанням закритого ключа підписувача виглядає наступним чином:

1. Вибирається випадкове ціле число k – разовий секретний ключ, де $0 < k < q$

2. Обчислюється $r = (g^k mod\ p)\ mod\ q$

3. Обчислюється $S = k^{-1}(h(M) + xr) mod\ q$, де $h(M)$ – значення хеш-функції $SHA{-}1$ від повідомлення M

4. Підписом для повідомлення M є пара (r, S)

4. Стандарт цифрового підпису DSS

Перевірка підпису

Перевірка підпису із використанням відкритого ключа підписувача виглядає наступним чином:

1. Обчислюється $w = s^{-1} \, mod \, q$

2. Обчислюється $u_1 = (h(M)w) \, mod \, q$

3. Обчислюється $u_2 = (rw) \, mod \, q$

4. Обчислюється $v = \left((g^{u_1} y^{u_2}) \, mod \, p\right) mod \, q$

5. Підпис дійсний, якщо $v = r$

4. Стандарт цифрового підпису DSS

Приклад 4.1: Підписати та перевірити підпис повідомлення M хеш-значення, якого $h(M) = 3$.

Генерація ключів

$p = 23, p - 1 = 23 - 1 = 22;$

$q = 11;$

$h = 2;$

$g = h^{(p-1)/q} \, mod \, p = 2^{22/11} mod \, 23 = 4;$

Закритий ключ: $x = 5;$

Відкритий ключ: $y = g^x \bmod p = 4^5 mod \, 23 = 1024 \, mod \, 23 = 12.$

4. Стандарт цифрового підпису DSS

Приклад 4.1: Підписати та перевірити підпис повідомлення M хеш-значення, якого $h(M) = 3$.

Підписування

Сесійний ключ: $k = 3$

$$r = (4^3 mod\ 23)\ mod\ 11$$
$$= 18\ mod\ 11 = 7$$

$$S = 3^{-1}(3 + 5 \cdot 7) mod\ 11 = 4$$
$$= 152\ mod\ 11 = 9$$

$3^{-1} mod\ 11 = 4$
(за розширеним алгоритмом Евкліда)

Перевірка підпису

Приймається $(M, 7, 9)$:

$$w = s^{-1}\ mod\ q = 9^{-1}\ mod\ 11 = 5$$
$$u_1 = 3 \cdot 5\ mod\ 11 = 4$$
$$u_2 = 7 \cdot 5\ mod\ 11 = 2$$

$$v = \big((4^4 \cdot 12^2)\ mod\ 23\big) mod\ 11$$
$$= 18\ mod\ 11 = 7$$
$$v = r$$