**Лабороторна работа №10**

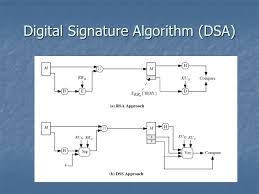
**Тема** криптоалгоритм “DSA”

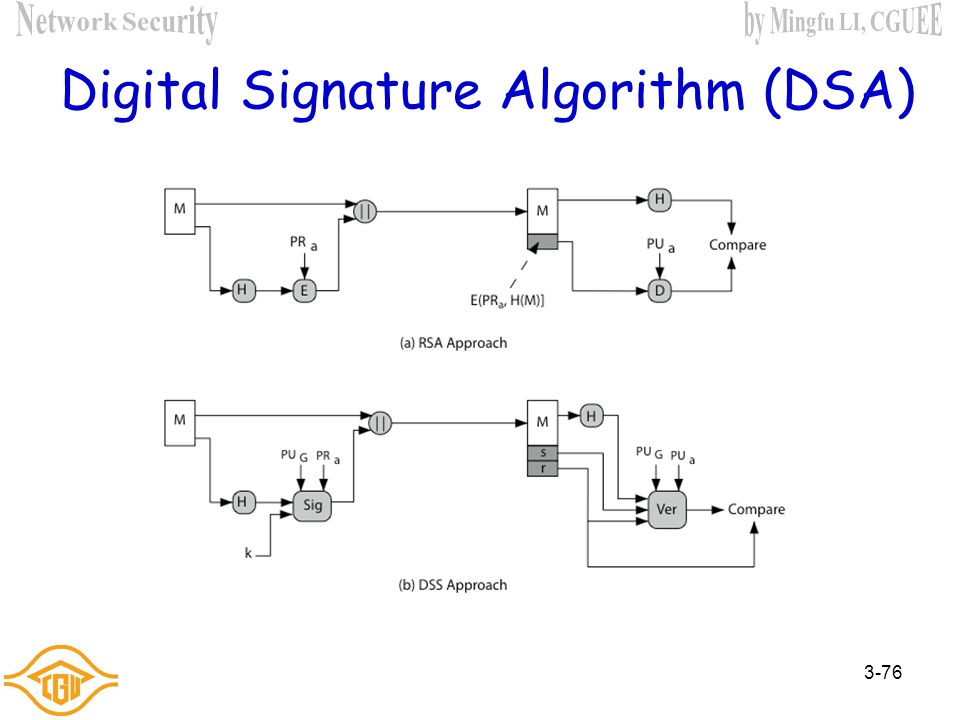
**Мета:** Практичне відпрацювання та закріплення теоретичних відомостей з криптоалгоритму “DSA”

DSA (Digital Signature Algorithm) - криптографічний алгоритм з використанням відкритого ключа для створення електронного підпису, але не для шифрування (на відміну від RSA і схеми Ель-Гамаля). Підпис створюється таємно, але може бути публічно перевірений. Це означає, що тільки один суб'єкт може створити підпис повідомлення, але будь-хто може перевірити її коректність. Алгоритм заснований на обчислювальній складності взяття логарифмів в кінцевих полях.

Алгоритм був запропонований Національним інститутом стандартів і технологій (США) в серпні 1991 і є запатентованим U.S. Patent 5 231 668, але НІСТ зробив цей патент доступним для використання без ліцензійних відрахувань. Алгоритм разом з криптографічного хеш-функцією SHA-1 є частиною DSS (Digital Signature Standard), вперше опублікованого в 1994 (документ FIPS-186 (Federal Information Processing Standards)). Пізніше були опубліковані 2 оновлені версії стандарту: FIPS 186-2 (27 січня 2000 року) і FIPS 186-3 (червень 2009).

Для підписування повідомлень необхідна пара ключів - відкритий і закритий. При цьому закритий ключ повинен бути відомий тільки тому, хто підписує повідомлення, а відкритий - будь-кому перевірити справжність повідомлення. Також загальнодоступними є параметри самого алгоритму. Для забезпечення такого доступу досить авторитетна організація (або кілька організацій) підтримує базу відповідності між реальними реквізитами автора (це може бути як приватна особа, так і організація) і відкритими ключами, а також всіма необхідними параметрами схеми цифрового підпису (використовувана хеш-функція). Ця організація також видає цифрові сертифікати.





Алгоритм DSA ґрунтується на труднощі обчислення дискретних логарифмів і є модифікацією класичної схеми Ель-Гамаля, де додано хешування повідомлення і додаткове порівняння **mod q**, яке дозволяє зробити підпис коротше. На основі схеми Ель-Гамаля побудовані й інші алгоритми, наприклад - російський ГОСТ 34.10-94, який зараз вважається застарілим. На зміну йому прийшов стандарт ГОСТ Р 34.10-2012, в якому використовується група точок еліптичної кривої.

Подібна модифікація, тобто перехід від мультиплікативної групи по модулю простого числа до групи точок еліптичної кривої існує і для DSA - ECDSA (англ. Elliptic Curve Digital Signature Algorithm - алгоритм цифрового підпису на еліптичних кривих). Він застосовується, наприклад, в криптовалюта bitcoin для підтвердження транзакцій. Цей переклад дозволяє зменшити розмір ключів без шкоди для безпеки - в системі bitcoin розмір закритого ключа 256 біт, а відповідного йому відкритого - 512 біт.

Інший поширений алгоритм з відкритим ключем (використовується і для шифрування, і для цифрового підпису), RSA (названий на честь авторів: Ривест, Шамір, Адлеман), заснований на складності факторизації великих чисел.

Параметри схеми цифрового підпису

Для побудови системи цифрового підпису потрібно виконати наступні кроки:

1. Вибір криптографічної хеш-функції ***H (x).***

2. Вибір простого числа ***q***, розмірність якого ***N*** в бітах збігається з розмірністю в бітах значень хеш-функції ***H (x)***.

3. Вибір простого числа ***p***, такого, що ***(p-1)*** ділиться на ***q***. Бітова довжина ***p*** позначається ***L (2 ^ L-1 <p <2 ^ L)***.

4. Вибір числа ***g*** такого, що його мультиплікативний порядок по модулю ***p*** дорівнює ***q***. Для його обчислення можна скористатися формулою ***g = h ^ (p-1) / q mod p***, де ***h*** - деяке довільне число, ***h*** Element of ***(1; p-1)*** таке, що ***g ≠ 1***. У більшості випадків значення ***h = 2*** задовольняє цій вимозі.

**Відкритий і секретний ключі**

1. Секретний ключ являє собою число ***x*** Element of ***(0, q)***

2. Відкритий ключ обчислюється за формулою ***y = g ^ x mod p***

Відкритими параметрачми є числа ***(p, q, g, y)***. Закритий параметр тільки один - число ***x***. При цьому числа ***(p, q, g)*** можуть бути загальними для групи користувачів, а числа ***x*** і ***y*** є відповідно закритим і відкритим ключами конкретного користувача. При підписуванні повідомлення використовуються секретні числа ***x*** і ***k***, причому число ***k*** має вибиратися випадковим чином (на практиці псевдовипадковим) при обчисленні підписи кожного наступного повідомлення.

Оскільки ***(p, q, g)*** можуть бути використані для декількох користувачів, на практиці часто ділять користувачів за деякими критеріями на групи з однаковими ***(p, q, g)***. Тому ці параметри називають доменними параметрами (Domain Parameters).

**Підпис повідомлення**

Підпис повідомлення виконується за наступним алгоритмом:

1. Вибір випадкового числа ***k*** Element of ***(0, q)***

2. Обчислення ***r = (g ^ k mod p) mod q***

3. Вибір іншого ***k***, якщо r = 0

4. Обчислення ***s = k ^ - 1 (H (m) + x \* r) mod q***

5. Вибір іншого ***k***, якщо ***s = 0***

6. Підписом є пара ***(r, s)*** загальної довжини ***2N***

Обчислювально складні операції це зведення в ступінь по модулю (обчислення ***g ^ k mod p***), для якого існують швидкі алгоритми , обчислення хешу ***H (x)***, де складність залежить від обраного алгоритму хешування і розміру вхідного повідомлення, і знаходження зворотного елемента ***k ^ - 1 mod q*** використовуючи, наприклад, розширений алгоритм Евкліда або малу теорему Ферма у вигляді ***k ^ - 1 mod q= k ^ q -2 mod q***.

**Перевірка підпису**

Перевірка підпису виконується за алгоритмом:

1. Обчислення  ***w = s ^ - 1 mod q***

2. Обчислення ***u1 = H (m) \* w mod q***

3. Обчислення ***u2 = r \* w mod q***

4. Обчислення ***v = (g ^ u1\* y ^ u2 mod p) mod q***

5 Підпис вірна, якщо ***v = r***

При перевірці обчислювально складні операції це два зведення в ступінь ***g ^ u1*** ***y ^ u2***, обчислення хешу ***H(x)*** і знаходження зворотного елемента ***s ^ - 1 mod q.*исновок:** Як видно з самого алгоритму, випадкові числа, що використовуються для створення цифрового підпису, відкриті. Це створює можливість для аналізу стійкості цих чисел. Цей факт свідчить на користь DSA, бо найбільш популярний алгоритм RSA зберігає генеровані прості числа у таємниці і перевірити їх можна лише знаючи приватний ключ. Отже алгоритм цифрового підпису DSA можна вважати більш стійким, ніж решта алгоритмів, що утворюють 128-бітовий хеш-образ (дайджест).