Лекція 11

ЦИФРОВИЙ ПІДПИС

В методі RSA відкритий ключ є відомим кожному. Тому кожен, хто знає відкритий ключ Боба, може надіслати йому шифроване повідомлення.

Припустимо, що Боб отримав зашифрованого листа, з якого можна зрозуміти, що він від Аліси. Використовуючи свій приватний ключ, Боб дешифрував це повідомлення:

(1) ЗУСТРІЧАЄМОСЬ О ВОСЬМІЙ АЛІСА

Чи може Боб *бути впевненим, що саме* Аліса *написала цього листа?*

Відповіддю на це питання є "ні", й це є серйозною проблемою, без розв'язання якої метод RSA є нікчемним.

З проблемою *аутентифікації* люди зустрічались протягом усієї своєї історії. Вона розв'язувалась різними засобами від особистих печаток до підпису. У сучасному світі для аутентифікації використовують сканування сітківки ока та відбитки пальців, але ці способи не підходять при листуванні, оскільки потребують особистої присутності особи. Чи існує спосіб аутентифікації електронних листів?

Над проблемою аутентифікації задумувались й автори RSA і саме вони вказали на спосіб її розв'язання в рамках свого методу.

---

[0] Printed from the file [cripto11.tex] on 26.12.2015

1. Метод RSA для цифрового підпису

Коли Аліса шифрує повідомлення для Боба, вона використовує його відкритий ключ. Щоб підписати своє повідомлення, Аліса використовує свій приватний ключ. Наприклад, якщо Аліса має

відкритий показник	відкритий модуль	приватний показник
k_A	n_A	j_A

то кожний символ $\mathcal{S}_{\mathtt{X}}$ свого підпису вона шифрує у символ цифрового підпису $\mathcal{H}_{\mathtt{X}}$ за допомогою формули

$$\mathcal{H}_{\mathtt{X}} \equiv (\mathcal{S}_{\mathtt{X}})^{j_A} \pmod{n_A}. \tag{2}$$

Так зашифрувати свій підпис може тільки Аліса, оскільки тільки вона знає свій приватний ключ.

Боб може прочитати підпис, використовуючи відкритий ключ Аліси: ①

$$\begin{aligned}(\mathcal{H}_{\mathtt{X}})^{k_A} &= \left((\mathcal{S}_{\mathtt{X}})^{j_A}\right)^{k_A} \pmod{n_A} = (\mathcal{S}_{\mathtt{X}})^{k_A j_A} \pmod{n_A} \\ &= \mathcal{S}_{\mathtt{X}} \pmod{n_A}.\end{aligned}$$

Приклад 1. Розглянемо детально формування повідомлення з цифровим підписом. Для цього використовуємо такі "іграшкові" ключи:

ім'я	відкритий показник	модуль	приватний показник
Аліса	3	85	43
Боб	3	187	107

[1] Пояснити останню рівність у наступному ланцюжку

Аліса надсилає повідомлення (1) й супроводжує його таким підписом

ЦЕ Я АЛІСА

В таблиці нижче показано процес шифрації частини повідомлення Аліси: перший рядок містить символи повідомлення, другий рядок — їхній цифровий еквівалент (позицію букви в алфавіті), а третій — коди, отримані за допомогою відкритого ключа Боба. Обчислення для третього рядка таблиці здійснено за правилом $\mathcal{C}_{\mathtt{X}} \equiv (\mathcal{P}_{\mathtt{X}})^3 \pmod{187}$:

(3)

$\mathcal{P}_{\mathtt{X}}$	З	У	С	Т	Р	І	Ч	А	Є	М	О	С	Ь
$\mathcal{D}_{\mathtt{X}}$	10	24	22	23	21	12	28	1	8	17	19	22	31
$\mathcal{C}_{\mathtt{X}}$	65	173	176	12	98	45	73	1	138	51	127	176	58

У наступній таблиці показано процес шифрації підпису Аліси: перший рядок містить символи підпису, другий рядок — їхній цифровий еквівалент (позицію букви в алфавіті), а третій — коди, отримані за допомогою приватного ключа Аліси. Обчислення для цифрового підпису Аліса здійснює за правилом: $\mathcal{H}_{\mathtt{X}} \equiv (\mathcal{S}_{\mathtt{X}})^{43} \pmod{85}$:

$\mathcal{S}_{\mathtt{X}}$	Ц	Е	Я	А	Л	І	С	А
$\mathcal{D}_{\mathtt{X}}$	27	7	33	1	16	12	22	1
$\mathcal{H}_{\mathtt{X}}$	3	48	67	1	16	23	28	1

Таким чином Аліса надсилає таке повідомлення Бобу:

(4)

65	173	176	12	98	45	73	1	138	51	127	176	58	
127	27	127	176	58	51	45	126	1	169	45	176	1	
3	48	67	1	16	23	28	1						

Перша частина цього повідомлення складається з двох рядків й містить шифр усієї фрази (1). Друга частина, яка

складається з одного (останнього) рядка, містить цифровий підпис.

Приклад 2. Коли Боб отримує листа, він починає дешифрацію: основну частину повідомлення за допомогою свого приватного ключа, а підпис — за допомогою відкритого ключа Аліси.

Таблиця нижче показує результат дешифрації листа (4), якого отримав Боб: індекс 1 у першому та другому рядках таблиці означає, що символи відносяться до першого рядку у листі, а індекс 2 — що символи відносяться до другого рядка у листі. Символом $\mathcal{D}_{\mathtt{X}}$ ми позначаємо номер позиції букви X в алфавіті (цифровий формат букви X). Дешифрацію Боб здійснює за правилом: $\mathcal{D}_{\mathtt{X}} \equiv (\mathcal{C}_{\mathtt{X}})^{107} \pmod{187}$:

$\mathcal{C}_{\mathtt{X}_1}$	65	173	176	12	98	45	73	1	138	51	127	176	58
$\mathcal{D}_{\mathtt{X}_1}$	10	24	22	23	21	12	28	1	8	17	19	22	31
$\mathcal{C}_{\mathtt{X}_2}$	127	27	127	176	58	51	45	126	1	169	45	176	1
$\mathcal{D}_{\mathtt{X}_2}$	19	3	19	22	31	17	12	14	1	16	12	22	1

Оскільки у таблиці (3) вже наведено буквенний еквівалент першого рядка, то перетворення у буквенний формат здійснимо тільки для другого рядка:

$\mathcal{D}_{\mathtt{X}_2}$	19	3	19	22	31	17	12	14	1	16	12	22	1
$\mathcal{P}_{\mathtt{X}_2}$	О	В	О	С	Ь	М	І	Й	А	Л	І	С	А

Щоб дешифрувати цифровий підпис, Боб використовує відкритий ключ Аліси; нижче показано результат його обчислень за правилом $\mathcal{S}_{\mathtt{X}} \equiv (\mathcal{H}_{\mathtt{X}})^3 \pmod{85}$:

$\mathcal{H}_{\mathtt{X}}$	3	48	67	1	16	23	28	1
$\mathcal{D}_{\mathtt{X}}$	27	7	33	1	16	12	22	1
$\mathcal{S}_{\mathtt{X}}$	Ц	Е	Я	А	Л	І	С	А

Тільки тепер Боб може бути вневненим, що лист йому надіслала саме Аліса.

2. Дайджест

Метод RSA розв'язує багато проблем, пов'язаних з секретністю ключів та інформації, яку необхідно передати від однієї сторони до іншої. По-перше, при використанні RSA немає питання про надійність обміну ключами, оскільки цей етап взагалі відсутній в RSA: будь-хто може надіслати шифрованого листа Бобу, оскільки кожен знає відкритий ключ Боба, але жодна третя сторона не може прочитати цього листа допоки приватний ключ Боба тримається в секреті.

Більше того, ніхто не може підробити підпис Аліси у її листі до Боба, оскільки ніхто, крім неї, не знає її приватного ключа. Чи це дійсно так?

Припустимо, що Боб отримав такого листа від Аліси разом з її цифровим підписом (ми наводимо листування у природному (буквенному) вигляді, оскільки нашою метою є пояснити проблему та шлях її подолання):

повідомлення: ВІДДАЙ ЕВІ ГРОШІ ЩО ТИ ВИНЕН МЕНІ
підпис: ЦЕ Я АЛІСА

Ми задаємо те ж питання, що й на початку лекції:

Чи може Боб *бути впевненим, що саме* Аліса *написала цього листа?*

Його сумніви пов'язані з тим, що Аліса перед цим листувалась з Євою. В одному з листів Аліси до Еви було використано її цифровий підпис:

повідомлення: ТИ ВЖЕ ПІДГОТУВАЛАСЬ ДО ІСПИТУ
підпис: ЦЕ Я АЛІСА

Тому Ева могла повторити цей підпис у листі до Боба, яке наведено вище. Таким чином, ніхто не може підробити цифровий підпис Аліси, але не виключено, що хтось має його копію і може її використати.

Щоб уникнути цієї проблеми, необхідно прив'язати цифровий підпис до змісту самого повідомлення: тоді кожного разу підпис буде іншим, що визначається самим повідомленням. Чи можна це зробити? Так, це можливо. Наприклад, підписом може служити саме повідомлення. Якщо k_B — це відкрита експонента Боба, а j_A — це приватна експонента Аліси, то Аліса своє повідомлення шифрує так:

лист шифрується з k_B: ВІДДАЙ ЕВІ ГРОШІ ЩО ТИ ВИНЕН МЕНІ
підпис шифрується з j_A: ВІДДАЙ ЕВІ ГРОШІ ЩО ТИ ВИНЕН МЕНІ

Зрозуміло, що такий спосіб не є економним. Загальноприйнятим підходом є використання *дайджеста*, тобто повторення повідомлення у скороченному (але все ж таки репрезентативному) вигляді. Наприклад, дайджестом у нашому прикладі може бути "слово", складене з кожного третього символа повідомлення (включно з пробілами між словами). Аліса включає дайджест ("слово" з підкреслених букв у першому рядку) у свій підпис:

лист шифрується з k_B: ВІДДАЙ␣ЕВІ␣ГРОШІ␣ЩО␣ТИ␣ВИНЕН␣МЕНІ
підпис шифрується з j_A: ДЙВГШЩТВМІ АЛІСА

Тепер сумнівів у Боба стосовно аутентичності не залишилось, оскільки своє повідомлення до Еви Аліса підписала зовсім іншим чином:

повідомлення: ТИ␣ВЖЕ␣ПІДГОТУВАЛАСЬ␣ДО␣ІСПИТУ
підпис: ␣ЕІОВА␣␣ПУ АЛІСА

Таким чином, копія цього підпису у листі до Боба означала б, що цей лист надсилала не Аліса.

2.1. Хеш функції. Формування дайджесту, розглянутого вище, можна описати математично. Розглянемо подальшу процедуру на прикладі повідомлення МИР, дайджестом якого є "слово" Р. Для отримання дайджесту, спочатку переведемо кожну букву у її числовий формат:

$$\text{М} \to 17, \qquad \text{И} \to 11, \qquad \text{Р} \to 21.$$

Утворимо число, записавши числові еквіваленти один за іншим:

$$m = 171121.$$

Тоді

$$m - \left[\frac{m}{100}\right] = 21 = \mathcal{D}_{\text{Р}}$$

є числовим кодом букви Р, яка входить в дайджест. ②

Дайджести для повідомлень можна утворювати різними способами, а не тільки тим, що ми використовували досі. У подальшому будемо вважати, що повідомлення записано у числовому вигляді, як пояснено вище. Таким чином, кожному повідомленню ми співставляємо певне число m.

В наступному означенні ми не формалізуємо вирази "*обчислити легко*", "*обчислити важко*", "*може трапитись дуже рідко*". У загальному випадку це зробити складно, але для конкретних прикладів ці вирази стають цілком зрозумілими.

[2] Аналогічним чином описати процедуру утворення дайджеста для "довгих" повідомлень

Означення 1. Відображення $H : \mathbf{N} \to \mathbf{N}$ ми називаємо *хеш-функцією*, якщо

1. значення $H(m)$, якщо задано m, обчислити легко;
2. значення m, якщо задано $H(m)$, обчислити важко;
3. рівність $H(m_1) = H(m_2)$ для $m_1 \neq m_2$ може трапитись дуже рідко.

Зауваження 1. Перші дві умови означення 1 свідчать, що H є односторонньою функцією (див. означення 9.1). Третя умова означає, що можна бути майже впевненим, що значення хеш-функції $H(m)$ "майже" визначає саме число m. Зверніть увагу, що третя умова означає, що все повідомлення можна "майже" замінити одним єдиним числом $H(m)$. Оскільки повідомлення однозначно описується числом m, то важливим є те, що $H(m)$ є значно меншим за m.

Фактично функції H з такими властивостями нам знайомі. Таким, наприклад, є дискретний логарифм. Відмінністю хеш-функцій від просто односторонніх є третя умова, яка означає, що H^{-1} не обов'язково є однозначною функцією.

Зауваження 2. Якщо H^{-1} є однозначною функцією, то рівність $H(m_1) = H(m_2)$ взагалі неможлива для $m_1 \neq m_2$. ③

Зауваження 3. Дайджест, який ми використовували досі, також є функцією від числового еквівалента повідомлення. Позначимо її через H. Ясно, що умова 1 означення 1 справджується для неї. Можна також погодитись, що й

[3] Чому рівність $H(m_1) = H(m_2)$ неможлива для $m_1 \neq m_2$, якщо H^{-1} є однозначною функцією?

умова 3 є вірною, умова ж 2 мабуть не є вірною для такої хеш-функції H.

В подальшому ми кажемо, про *колізію*, якщо рівність $H(m_1) = H(m_2)$ можлива для $m_1 \neq m_2$.

Зауваження 4. Колізії можуть виникати й для добре відомих функцій, наприклад $H(x) = H(-x)$ для $H(x) = x^2$.

Правило 1. Хеш-функції для цифрового підпису

для цифрового підпису необхідно використовувати хеш-функції; при виборі H необхідно досягти компромісу між величиною значень $H(m)$ (їх необхідно робити якомого меншими) та частотою виникнення колізій (їхню кількість необхідно зменшити; для цього необхідно розширити область значень для H; значення $H(m)$ можуть зростати).

---

3. Сліпий цифровий підпис

Розглянемо ще один аспект цифрового підпису та застосування ідеї RSA. Автором підходу, розглянутого нижче, є американський криптолог Девід Чаум.

Припустимо, що `Аліса` бажає, щоб

(w_1) `Боб` поставив свій підпис під її повідомленням.

Додатковим її бажанням є те, що

(w_2) `Боб` не зможе прочитати саме повідомлення, навіть якщо він залишить собі його копію.

Такі ситуації є доволі розповсюдженими між бізнес партнерами, коли один з них робить пропозицію іншому й бажає,

щоб цей факт було засвідчено нотаріусом (важливими є також дата та час, коли ця пропозиція зроблена). Умовою обох партнерів є те, що нотаріус не бачить суми, яку один з них пропонує іншому. Таким чином, нотаріус засвідчує документ "всліпу", що й пояснює назву такого підпису.

Чи можна задовольнити ці дві вимоги `Аліси`?

Приклад 3. Розглянемо модель нашої ситуації, для якої поставлену задачу можна розв'язати. Уявімо, що в конверті знаходиться документ і копіювальний лист. Якщо нотаріус підписує конверт, то його підпис відбивається на документі. Відкривши конверт, отримуємо підписаний нотаріусом документ, причому його зміст, як і раніше, нотаріусу невідомий.

Чи можна описати модель з приклада 3 у математичних термінах? Якщо `Боб` (нотаріус) має відкритий ключ n_B та k_B (модуль та експонентау), то фактично `Аліса` бажає, щоб `Боб` поставив цифровий підпис з використанням n_B та k_B. Тоді, у разі потреби, кожен зможе пересвідчитись, що саме `Боб` завізував повідомлення. ④

3.1. Вимоги до схеми сліпого підпису. Будь-яка схема безпечного сліпого підпису повинна мати наступні дві властивості.

1) *Нульове розголошення.* Ця властивість означає, що `Аліса` отримує підпис `Боба` на своєму повідомленні, не розкриваючи його змісту.
2) *Абсолютна впевненість.* Ця властивість означає, що тільки `Боб` може сгенерувати електронний підпис.

[4] Як можна пересвідчитись, що саме `Боб` завізував повідомлення?

Цим двом вимогам задовольняє наступна схема сліпого електронного підпису, у якій (n, k) — це відкритий ключ Боба, а j — його приватний ключ.

Алгоритм 1. Сліпий цифровий підпис

1. Аліса переводить своє повідомлення у числовий формат m;
2. Аліса обирає $0 < \ell < n$, для якого $(\ell, n) = 1$;
3. Аліса знаходить $i = \ell^{-1} \pmod{n}$;
4. Аліса маскує своє повідомлення $\mathtt{blind}(m) \stackrel{\text{def}}{=} t = m\ell^k \pmod{n}$;
5. Боб підписує замасковане повідомлення за допомогою свого приватного ключа, тобто Боб обчислює
   $\mathtt{sign}(\mathtt{blind}(m)) \stackrel{\text{def}}{=} y = t^j \pmod{n}$;
6. Аліса демаскує повідомлення з підписом,
   тобто обчислює $z = yi \pmod{n}$.

3.2. Доведення алгоритму 1. Щоб зрозуміти алгоритм 1, перш за все встановимо чому дорівнює число z, обчислене на шостому кроці:

$$\begin{aligned} z &= yi \pmod{n} = t^j i \pmod{n} = \left(m\ell^k\right)^j i \pmod{n} \\ &= m^j \ell i \pmod{n} \qquad ⑤ \\ &= m^j \pmod{n}. \qquad ⑥ \end{aligned}$$

Таким чином, z — це повідомлення Аліси, зашифроване приватним ключем Боба. Це доводить, що тільки Боб міг завізувати документ m, оскільки ніхто інший не знає j.

[5] пояснити цю рівність!
[6] пояснити цю рівність!

Аліса зберігає z і у будь-який момент може довести, що Боб завізував документ. ⑦

Боб не може прочитати документ m на кроці 5, оскільки він отримує лише t, з якого не можна відтворити m у легкий спосіб. ⑧

Приклад 4. Аліса робить пропозицію Валерії вартістю 1000 доларів. Аліса бажає, щоб її агент Боб засвічив її пропозицію, але не бажає, щоб він бачив саму суму. Боб має відкритий ключ $(n, k) = (5561, 235)$.

1. Повідомленням Аліси є $m = 1,000$. Вона обирає випадкове число $\ell = 91$ й знаходить i, обернене до ℓ за модулем n, тобто $i = 550$. ⑨ Тепер Аліса маскує свою пропозицію, обчислюючи

$$t \equiv m\ell^k \pmod{n} = 1,000 \times 91^{235} \pmod{5561} = 1715. \quad ⑩$$

2. Боб підписує всліпу замасковане повідомлення t, використовуючи для цього свій приватний ключ (n, j) й обчислюючи

$$y \equiv t^j \pmod{n} = 1715^j \pmod{5561} = 216.$$

Зауважте, що Боб не відкриває свій приватний ключ j під час цієї процедури. ⑪

---

[7] Яким чином Аліса може довести, що саме Боб завізував документ?

[8] Чому Боб не може у легкий спосіб прочитати документ m на кроці 5?

[9] Перевірити, що $550 \times 91 \equiv 1 \pmod{5561}$.

[10] Довести, що $t \equiv 1715 \pmod{5561}$.

[11] Спробуйте визначити приватний ключ Боба.

3. Зрозуміло, що

$$y \equiv t^j \pmod{n} = (m\ell^k)^j \pmod{n} = m^j \ell \pmod{n}. \qquad ⑫$$

Тепер `Аліса` знімає маску, домноживши на обернене до ℓ за модулем n:

$$z \equiv yi \pmod{n} = 216 \times 550 \pmod{5561} = 2019. \qquad ⑬$$

4. `Валерія` може прочитати повідомлення `Аліси`, якщо використає відкритий ключ `Боба` й обчислить

$$m \equiv z^k \pmod{n} = 2,019^{235} \pmod{5561} = 1000. \qquad ⑭$$

Ніхто, крім `Боба` (навіть читач цих рядків!), не знає його приватний ключ (n, j). Тому, поки число $n = 5561$ не факторизовано, ніхто не знає j. ⑮

4. Застосування схеми сліпого підпису

4.1. Електронні гроші. Для багатьох з нас готівка має кілька привабливих рис, серед яких

i) нею легко розраховуватись,
ii) вона є ананімною у тому розумінні, що нею можна розраховуватись не називаючи себе.

---

[12] Пояснити останню рівність.
[13] Перевірити рівність $z = 2019$.
[14] Перевірити обчислення `Валерії`.
[15] Факторизувати число 5561 й визначити j.

Д. Чаум запропонував криптографічну схему функціонування електронних грошей, яка також має зазначені риси. Спочатку розглянемо наступну ілюстративну модель електронних грошей, запропоновану Чаумом.

Припустимо, що `Аліса` бажає отримати від банку чек вартістю 20 гривень. Вона також бажає, щоби банк не дізнався яким чином і коли вона використає цей чек.

Модель Чаума для електронних грошей

1. `Аліса` отримує в банку чистий аркуш паперу, обирає випадкове число й записує його на цьому аркуші. Це число будемо називати серійним номером чеку.
2. `Аліса` вкладає цей аркуш разом з копіркою у конверт і звертається до банківського співробітника.
3. Він ставить спеціальну печатку на конверті, яка свідчить, що чек в конверті вартує саме 20 гривень. Крім цього, співробітник банку переводить 20 гривень з рахунку `Аліси` на спеціальний рахунок, який використовується для електронних розрахунків всіх клієнтів банку (ця операція називається *дебетуванням* рахунку).
4. `Аліса` дістає аркуш з відбитком банківського штампу й розраховується ним у магазині.
5. Продавець надсилає чек до банку. Банк перевіряє чи надсилався раніше чек з таким серійним номером. Якщо чек з таким номером надійшов вперше, то банк переказує 20 гривень з спецрахунку на рахунок продавця (ця операція називається *кредитуванням* рахунку) й вносить номер чеку до списку сплачених чеків.

Оскільки банк не знав серійний номер до надходження чеку до банку, він не знає хто саме скористався таким чеком, тобто ананімність `Аліси` збережено.

Зауваження 5. Припустимо, що разом з `Алісою` аналогіч-

ний чек отримав Боб. Якщо так трапиться, що вони впишуть однаковий серійний номер у свої чеки, то пізніше один з них не зможе ним розрахуватись. ⑯ Щоб уникнути такої неприємної події, банк може вимагати від клієнтів обирати дуже великі випадкові числа (наприклад, з проміжку від 10^{100} до $10^{101}-1$). В цьому випадку ймовірність співпадіння двох номерів є майже нулевою.

Нижче наведено алгоритм, який реалізує у цифровому вигляді модель, описану вище.

Алгоритм 2. Електронні гроші

1. Аліса обирає серійний номер S й маскуючий коефіцієнт ℓ; перші цифри в S ідентифікують банк, всі решта обираються випадково. Аліса також обчислює $i \equiv \ell^{-1} \pmod{n}$.
2. Аліса маскує серійний номер, обчислюючи $y \equiv S\ell^k \pmod{n}$; значення y вона надсилає до банку.
3. Банк дебетує рахунок Аліси на 20 гривень й підписує замаскований серійний номер, обчислюючи $t \equiv y^j \pmod{n}$; це значення банк повертає Алісі.
4. Аліса знімає своє маскування, обчислюючи $z \equiv ti \pmod{n}$; при купівлі вона повідомляє z продавцю.
5. Продавець обчислює $S \equiv z^k \pmod{n}$; за першими цифрами S продавець ідентифікує банк й надсилає туди S.
6. Банк перевіряє серійний номер S й кредитує рахунок продавця на 20 гривень.

[16] Пояснити цю обставину.

В алгоритмі 2 ми вважаємо, що (n, k) — це відкритий ключ, а j — це приватний ключ, які банк використовує для чеків вартістю 20 гривень.

Зауважимо, що на кроці 4 описаної процедури `Аліса` фактично обчислює

$$z \equiv ti \pmod{n} = y^j i \pmod{n} = (S\ell^k)^j i \pmod{n}$$
$$= S^j \ell i \pmod{n} = S^j \pmod{n},$$

тобто серійний номер, зашифрований приватним ключем банка. Це обчислення пояснює результат на кроці 5. ⑰

4.2. Таємне голосування. Ідея сліпих цифрових підписів використовується для організації таємного голосування. Опишемо один з підходів, опублікований в 1992 році японськими вченими А. Фудзіока, Т. Окамото та К. Охта. Термінологія, яку ми використовуємо нижче ("маскування", "підпис" тощо), є зрозумілою з алгоритма 1.

Виборець шифрує свій вибір за допомогою приватного ключа і маскує його. Після цього вписує результат у бюлетень, підписує і надсилає його у контрольну комісію. Контрольна комісія перевіряє підпис і встановлює, що він належить зареєстрованому виборцю, який ще не голосував.

Якщо виборчий бюлетень дійсний, комісія підписує виборчий бюлетень і повертає його виборцю. Зауважимо, що комісія не може встановити уподобання виборця, вона тільки може перевірити його підпис під бюлетенем. Отримавши бюлетень з підписом комісії, виборець видаляє своє маскування і надсилає цей варіант бюлетеня в рахункову комісію, яка перевіряє підпис контрольної комісії.

[17] Перевірити обчислення на кроці 5.

Якщо виборчий бюлетень є дійсним, лічильна комісія зберігає його для подальшої обробки. Відзначимо, що в цей момент рахункова комісія не може прочитати результат голосування данного виборця. В узгоджений момент виборець надсилає свій ключ в лічильну комісію для дешифрації. Тільки тепер комісія може визначити вподобання виборця.

Передбачається, що виборець на кожному етапі має можливість контролювати статус свого бюлетеня.

Як і у випадку сліпих підписів, жодна з комісій не має змоги визначити уподобання виборця допоки він сам не надішле свій ключ.

4.3. Захист пароля. Для ідентифікації часто використовують паролі або PIN (Personal Identification Number). Паролі зазвичай передаються хост-комп'ютеру через захищені лінії зв'язку; компьютер порівнює пароль з тими, що зберігаються в його списку.

Такі системи ідентифікації мають вразливі сторони, однією з яких є потенційна можливість отримати несанкціонований доступ до списку паролів. Цей недолік можна усунути за допомогою метода з використанням односторонньої функції. Цей метод передбачає, що зберігаються не самі паролі, а лише значення односторонньої функції, аргументами якої є паролі.

Наприклад, якщо паролем є число x, то комп'ютер може зберігати $H(x) = a^x \pmod{n}$, де a та n фіксовані великі числа. Всякий раз, коли ви повідомляєте свій пароль x, обчислюється значення $H(x)$, яке порівнюється з записами у базі даних. Якщо порівняння успішне, ви пройшли етап ідентифікації.

Якщо зловмисник отримує несанкціонований доступ до

бази даних, він не може обчислити ваш пароль, оскільки це еквівалентно обчисленню дискретного логарифма, що, як ми знаємо, є складною операцією. Отже, ваш пароль захищений від несанкціонованого доступу до списку паролів.

Зауважимо також, що паролі, які передаються каналами голосового зв'язку, є уразливими для прослуховування. Якщо хтось зміг підслухати ваш пароль, коли ви називали його по телефону, то пізніше зловмисник може намагатись видавати себе за вас, використовуючи підслуханий пароль.

5. Електронний підпис для схеми Ель-Гамаля

Особливістю криптосистеми Ель-Гамаля (розділ 10.6) є наявність ефективної процедури цифрової перевірки особи (*аутентифікації*) кореспондента. Нехай `Аліса` використовує систему Ель-Гамаля з відкритим ключем (p, r, a) та приватним ключем key k. Припустимо, що вона надсилає `Бобу` повідомлення M. Щоб запевнити `Боба` у тому, що саме вона є автором повідомлення, `Аліса` створює цифровий підпис. Для цього вона спочатку знаходить число $1 \le j \le p-1$ з $(j, p-1) = 1$. Далі вона обчислює

$$c \equiv r^j \pmod{p}, \qquad 0 \le j \le p-1.$$

Після цього вона обирає довільну частину повідомлення, наприклад, перший блок B, й знаходить розв'язок лінійної конгруенції

$$jd + kc \equiv B \pmod{p-1}, \qquad 0 \le d \le p-2.$$

Метод розвязання цієї конгруенції описано в розділі 4.2. Пара цілих чисел (c, d) і є цифровим підписом, який додається

до повідомлення. Його може створити тільки той, хто знає приватний ключ k, випадкове ціле число j та саме повідомлення M. Боб за допомогою відкритого ключа Аліси (p, r, a) перевіряє підпис. Для цього він підраховує два числа

$$V_1 \equiv a^c c^d \pmod{p}, \qquad V_2 \equiv r^B \pmod{p},$$

$0 \le V_1, V_2 \le p - l$. Цифровий підпис приймається, якщо $V_1 = V_2$. Це випливає з наступних конгруенцій

$$V_1 \equiv a^c c^d \equiv (r^k)^c (r^j)^d \equiv r^{kc+jd} \equiv r^B \equiv V_2 \pmod{p}.$$

⑱ Зауважимо, що ця процедура аутентифікації цифрового підпису не вимагає знання приватного ключа k.

Приклад 5. Аліса використовує криптосистему Ель-Гамаля з відкритим ключем $(43, 3, 22)$ та приватним ключем $k = 15$. Вона бажає надіслати Бобу повідомлення з своїм цифровим підписом. Для цього вона спочатку обирає ціле число $0 \le j \le 42$ з $(j, 42) = 1$, наприклад $j = 25$. Якщо першим блоком повідомлення є $B = 13$, то вона підраховує

$$c \equiv 325 \equiv 5 \pmod{43},$$

а після цього розв'язує лінійну конгруенцію

$$25d \equiv 13 - 5 \cdot 15 \pmod{42}$$

(розв'язком її є $d \equiv 16 \pmod{42}$). ⑲ Пара $(5, 16)$ являє собою цифровий підпис Аліси. Отримавши повідомлення,

[18] Пояснити чому звідси випливає, що $V_1 = V_2$.

[19] Впевнитись, що $d = 16$ є розв'язком конгруенції $25d \equiv 13 - 5 \cdot 15 \pmod{42}$.

Боб перевіряє підпис, порівнюючи два цілих числа V_1 таV_2:

$$V_1 \equiv 22^5 \cdot 5^{16} \equiv 39 \cdot 40 \equiv 12 \pmod{43},$$
$$V_2 \equiv 3^{13} \equiv 12 \pmod{43}.$$

6. Контрольні питання

1. Пояснити останню рівність у наступному ланцюжку (стор. 251).
2. Аналогічним чином описати процедуру утворення дайджеста для "довгих" повідомлень (стор. 256).
3. Чому рівність $H(m_1) = H(m_2)$ неможлива для $m_1 \neq m_2$, якщо H^{-1} є однозначною функцією? (стор. 257).
4. Як можна пересвідчитись, що саме Боб завізував повідомлення? (стор. 259).
6. пояснити цю рівність! (стор. 260).
6. пояснити цю рівність! (стор. 260).
7. Яким чином Аліса може довести, що саме Боб завізував документ? (стор. 260).
8. Чому Боб не може у легкий спосіб прочитати документ m на кроці 5? (стор. 261).
9. Перевірити, що $550 \times 91 \equiv 1 \pmod{5561}$. (стор. 261).
10. Довести, що $t \equiv 1715 \pmod{5561}$. (стор. 261).
11. Спробуйте визначити приватний ключ Боба. (стор. 261).
12. Пояснити останню рівність. (стор. 261).
13. Перевірити рівність $z = 2019$. (стор. 262).
14. Перевірити обчислення Валерії. (стор. 262).
15. Факторизувати число 5561 й визначити j. (стор. 262).
16. Пояснити цю обставину. (стор. 263).
17. Перевірити обчислення на кроці 5. (стор. 265).
18. Пояснити чому звідси випливає, що $V_1 = V_2$. (стор. 268).
19. Впевнитись, що $d = 16$ є розв'язком конгруенції $25d \equiv 13 - 5 \cdot 15 \pmod{42}$. (стор. 268).

БІОГРАФІЇ

Чаум, *Девід* (нар. 1955 р.), американський криптограф, автор чисельних криптографічних протоколів, серед яких `ecash` та `DigiCash`. Його робота "*Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*", опублікована в 1981 році, стала основою для багатьох досліджень та розробок у галузі анонімного обміну даними. Ідею сліпого підпису обгрунтував в роботі 1982 року.

В 1989 році він (разом з Хансом ван Антверпеном) описав протокол так званих *незаперечних підписів*. Особливість процесу верифікації такого цифрового підпису полягає у тому, що верифікацію може здійснити не кожен користувач. Такі підписи ставлять розробники програмного забезпечення, для того, щоб тільки зареєстровані користувачі могли перевірити підпис (що може означати, що тільки після реєстрації/придбання з'являється можливість користуватись даним програмним продуктом).

В 1991 році він (разом з Юджином ван Хейстом) розробив протокол так званих групових підписів, який дозволяє кожному члену групи анонімно підписати повідомлення від імені всієї групи. При цьому керівник групи має право відкликати анонімність будь-кого з підписантів у разі виникнення суперечок.

Чаум є відомим також своїм визначним внеском у розробку безпечних систем голосування. В 2011 році Чаум висловив ідею рандомізованих виборів, основану на випадковому формуванні груп виборців з збереженням анонімності. При цьому результат голосування цієї групи є репрезентативним для популяції, з якої було обрано виборців.

Він є також автором концепції *доведень з нульовим знанням*. Приклад для цієї концепції можна знайти у середньовічній математиці. В 1535 році Нікола Тарталья проголосив, що знає загальну формулу для розв'язків кубічного рівняння $ax^3 + bx^2 + cx + d = 0$. Він так і не опублікував цю формулу, хоча беззаперечно довів, що володіє нею, оскільки зміг розв'язати велику кількість кубічних рівнянь, запропонованих йому опонентами.