Лекція 10

КРИПТОСИСТЕМИ З ВІДКРИТИМ КЛЮЧЕМ

Існують два типи криптографії: та, що дозволяє тобі мати секрети від твоєї молодшої сестри, й та, що дозволяє мати секрети від твого уряду.

Б. Шнайер, криптограф

Слідуючи традиції та загальноприйнятій практиці, надалі сторони, які приймають участь у шифрованому листуванні, називаються `Алісою` та `Бобом`.

Для приватного листування між `Алісою` та `Бобом` вистачає простих шифрів, які ми вивчали у попередніх лекціях. Для збереження інформації в секреті `Аліса` та `Боб` можуть домовитись про, наприклад, використання експоненціального $E_{k,n}$ шифру з фіксованими параметрами k та n, які є невідомими для інших осіб. Щоб підтримувати секретність, ці значення необхідно змінювати час від часу. Конфеденційність є найменшою в той момент, коли `Аліса` та `Боб` обмінюються цими параметрами.

Уявімо тепер, що `Аліса` має листуватись з багатьма іншими особами (`Алісою` може, наприклад, бути великий банк). В такому випадку цілком слушною стратегією для `Аліси` є надати кожному зі своїх кореспондентів унікальні параметри k та n. Але в цьому випадку їй необхідно мати список

[0] Printed from the file `[cripto10.tex]` on 26.12.2015

цих параметрів, щоб не переплутати їх при листуванні з кореспондентами. Наявність такого списку підвищує ризик втрати конфеденційності, оскільки список можна вкрасти або прочитати його з компьютера, якщо він зберігається у файлі.

Таким чином, найбільш уразливими етапами секретного листування є обмін ключами та збереження ключів у тайні.

1. Головоломки Р. Меркла

Припустимо, що `Аліса` і `Боб` хотіли б приховати від інших зміст свого листування. Щоб запобігти втраті конфеденційності під час обміну ключами, `Боб` надсилає до `Аліси` велику кількість головоломок, кожну з яких вона в змозі розв'язати за помірний час. Ці головоломки можуть бути зашифрованими повідомленнями з невідомими ключами. `Аліса` обирає випадковим чином одну з них і розв'язує її (методом грубої сили). Тепер `Аліса` та `Боб` можуть спілкуватись, оскільки обидва знають ключ. Жоден зловмисник не може прочитати їхні повідомлення, оскільки не знає яку з головоломок обрала `Аліса`. Щоб отримати код, зловмисник має розв'язати *всі* головоломки, але для цього потрібно набагато більше часу, ніж витратила `Аліса`. Через певний час `Боб` та `Аліса` можуть повторити процедуру вибору ключа й не хвилюватись, що зловмисник має доступ до їхнього листування.

Описаний підхід до вибору ключів запропонував (саме в такій формі) в 1974 році Роберт Меркл; його метод було опубліковано через 4 роки потому.

2. Метод В. Діффі та М. Хеллмана

В 1976 році Вітфілд Діффі та Мартін Хеллман опублікували роботу, у якій запропонували революційний спосіб обміну ключами по несекретним каналам, який вони назвали *методом відкритих ключів*. Кожен з користувачів криптосистеми, яку описали Діффі та Хеллман, має два ключі: *приватний* та *відкритий*.

Приватний ключ тримається в секреті й ніколи никому не повідомляється. Жодних захисних дій стосовно збереження секретності відкритого ключа не здійснюється; вважається, що він є відомим всім, в тому числі й зловмисникам.

Якщо `Аліса` хоче надіслати `Бобу` повідомлення, вона використовує його відкритий ключ. Для того, щоб його прочитати, `Боб` використовує свій приватний ключ. Хоча ці ключі й пов'язані один з іншим, не існує можливості дізнатися про приватний ключ за допомогою відкритого. Тому третя сторона не зможе прочитати листи від `Аліси` до `Боба`.

Зауваження 1. Всі шифри, які вивчались у попередніх лекціях, мали лише один, секретний, ключ. Кожне повідомлення, зашифроване за допомогою цього ключа, можна було розшифрувати за допомогою іншого ключа, який однозначно обчислювався з секретного.

Наприклад, число a є ключем для мультиплікативного шифру $M_{a,33}$, яке використовують для шифрування повідомлень за формулою (3.1). Для дешифрації повідомлення (див. формулу (3.6)) необхідно знання оберненого за модулем числа $a^{-1} \pmod{33}$, яке однозначно обчислюється за секретним ключем a.

Зверніть увагу на наступну обставину. Оскільки відкритий ключ у системі Діффі–Хеллмана є загально відомим,

будь-хто, не тільки Аліса, може надіслати Бобу шифроване повідомлення.

Така ж ситуація спостерігається у кожному з парадних багатоповерхівок: будь-хто може залишити листа Бобу, вкинувши лист у поштову скриньку Боба. З іншого боку, тільки Боб може дістати листа зі скриньки, оскільки тільки Боб має ключ від неї. У даному випадку, ключ від поштової скриньки грає роль приватного ключа в системі Діффі–Хеллмана, а отвір в поштовій скриньки — роль відкритого ключа.

Чи можна аналогічну ситуацію змоделювати в криптографії? Іншими словами, чи можна практично реалізувати ідею Діффі–Хеллмана?

3. Шифр RSA

Після виходу з друку статті Діффі та Хеллмана, їхніми ідеями зацікавились Рональд Рівест та Аді Шамір з Масачусетського технологічного інституту. Присвятивши певний час реалізації ідеї Діффі–Хеллмана, вони знайшли спосіб її реалізації. Свої розробки вони показали своєму колезі Леонарду Еделману, який водночас знайшов помилку у їхніх міркуваннях. Наступна спроба Рівеста та Шаміра також мала вади, на які вказав той же Еделман. Ця історія повторювалась 42 рази й лише на 43-ій спробі Еделман визнав, що помилки не існує.

В 1978 році вийшла спільна стаття трьох співавторів, Рівеста, Шаміра та Еделмана з описом методу, який зараз називається *шифром RSA*, що є абревіатурою за першими буквами їхніх прізвищ, написаних англійською мовою. Шифр RSA не тільки став першим прикладом системи з відкритими ключами, але й зберігає популярність донині.

3.1. Що таке шифр RSA. RSA — це експоненціальний шифр з модулем, який дорівнює добутку двох простих чисел, тобто $n = pq$. Саме такі шифри ми вивчали у лекціях 8 та 9. З 1978 року числа, які дорівнюють добутку двох простих, називають *RSA числами*.

Є одна принципова властивість RSA шифру, яка вирізняє його серед інших шифрів $E_{k,n}$, а саме:

Правило 1. Властивість RSA шифру

не тільки модуль $n = pq$ шифру RSA має бути дуже великим, але й його прості дільники p та q мають бути дуже великими.

Кожен $E_{k,n}$ є шифром з приватним ключем (k, n): це зовсім просто зрозуміти, якщо n є простим числом або $n = pq$. Дійсно, в цих випадках дешифрація здійснюється за допомогою показника кореня $k^{-1} \pmod{\phi(n)}$ (див. правила 1 та 2 в лекції 8).

Чи може в такому разі $E_{k,n}$ бути ще й шифром з відкритим ключем?

Знаходження оберненого числа за модулем є відносно швидкою операцією. У прикладі 9.1 ми показали процес дешифрації для RSA з $k = 1649$ та $n = 5251$. Оскільки n не є надто великим, його факторизація є простою: $5251 = 59 \cdot 89$. Подальші обчислення у прикладі 9.1 також були досить простими.

Схожу задачу ми розв'язували у прикладі 9.5. В цьому випадку $k = 3$, а $n = 15,002,557$. Ми вказали без обчислень, що $15,002,557 = 2447 \cdot 6131$. Перевірка цієї рівності

є простою задачею, ① але як встановити цю факторизацію, якщо її не знати зазделегідь?

В розділі 9.3 ми відзначили, що факторизація великих чисел є складною операцією. Саме ця обставина дозволяє застосовувати RSA шифр.

3.2. Відкритий та приватний ключі для RSA. Для дешифрації повідомлення, закодованого за допомогою $E_{k,n}$ шифру, необхідно обчислити обернене за модулем число

$$j = k^{-1} \pmod{\phi(n)}$$

(див. формулу (8.4)).

Для RSA шифру $\phi(n) = (p-1)(q-1)$ ②, тобто знання p та q дає змогу обчислити $\phi(n)$, а потім й обернене число $k^{-1} \pmod{\phi(n)}$. Якщо p та q є дуже великими числами, то знання їхнього добутку pq не дозволяє швидко знайти дільники p та q (згадайте історію про число RSA-640 в прикладі 9.6). Ми повернемося до питання складності факторизації нижче у §3.3.

Термінологія у випадку RSA шифру трохи змінюється: числа k та j у випадку шифру RSA називають *відкритою експонентою* та *приватною експонентою* (або *відкритим ключем* та *приватним ключем*). Як зрозуміло з назв, k є відомим числом, а j — секретним. Тим не менше, для їхнього добутку справджується ключова властивість ③

$$a^{kj} \equiv a \pmod{n} \qquad \text{для всіх } a.$$

[1] Перевірте ще раз!
[2] Пригадайте, чому $\phi(n) = (p-1)(q-1)$?
[3] Пригадайте, чому ця властивість є вірною?

Немає жодної потреби вимагати, щоб k було дуже великим числом, ④ тому часто обирають $k = 3$ (це полегшує шифрацію повідомлень).

Правило 2. Відкритий та приватний ключі для RSA

Таким чином, відкритим ключем RSA шифру є пара чисел k та n, а приватним — число j. Можна також вважати, що приватним шифром є пара чисел p та q, причому $n = pq$. ⑤

3.3. Надійність RSA. З попереднього обговорення випливає, що для безпеки RSA-криптосистеми важливо правильно вибрати прості числа p і q. Якщо вони малі, то система легко зламується. Проте недостатньо вибрати великі p і q: навіть якщо p і q величезні, але різниця $|p - q|$ мала, їхній добуток $n = pq$ легко розкладається на множники (див. задачу 13).

Поняття складності операції можна інтуітивно зрозуміти на такому прикладі. Припустимо, що однієї секунди вистачить, що прочитати вголос всі цифри від 0 до 9. Оскільки чисел від 0 до 99 в 10 разів більше, то необхідно 10 секунд, щоб їх прочитати вголос. У загальному випадку, додавання однієї додаткової цифри до десяткового представлення числа збільщує час читання в 10 разів. Подивіться на наступну таблицю, яка показує як зростає час для здійснення операції читання вголос при додаванні додаткової цифри:

[4] Пояснити, чому не обов'язково вимагати, щоб k було дуже великим числом?

[5] Чи дійсно знання j є еквівалентним до знання (p, q)?

додаткові цифри	час (у секундах)	час в інших одиницях
1	10	
2	100	$\approx$ 1.5 мін.
3	1,000	15 мін.
4	10,000	2.5 год.
5	100,000	1 день
6	1,000,000	10 днів
7	10,000,000	100 днів
8	100,000,000	$\approx$ 3 роки
9	1,000,000,000	30 років
10	10,000,000,000	300 років

Таким чином, додавання лише 10 додаткових цифр змінює час виконання операції від 1 секунди до 300 років!

3.4. Початок історії RSA. Робота Рівеста, Шаміра, Еделмана з'явилась у 1978 році, але увага до шифру RSA виникла роком раніше. В 1977 році популяризатор науки Мартін Гарднер у своїй постійній рубриці "*Математичні ігри*" (!) у журналі *Scientific American* опублікував число

RSA-129 = 1143816257 5788886766 9235779976 1466120102 1829672124
2362562561 8429357069 3524573389 7830597123 5639587050
5898907514 7599290026 879543541

та зашифрований за його допомогою текст

9686	9613	7546	2206
1477	1409	2225	4355
8829	0575	9991	1245
7431	9874	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	8013	3919	9055
1829	9451	5781	5154

за дешифрацію якого пропонувалась премія в \$100.

Гарднеру цю головоломку запропонували автори шифру RSA. Рон Рівест, один з авторів RSA, оцінив час, потрібний для дешифрації: він вважав, що дешифрація стане можливою не раніше, ніж через $40 \cdot 10^{15}$ років. Це означало, що фактично він не сподівався на те, що число RSA-129 взагалі можна факторизувати.

Повідомлення було дешифровано через 17 років, коли група з 600 ентузіастів та їхні 1600 компьютерів змогли факторизувати RSA-129 за 8 місяців неперервної роботи. Це стало можливим завдяки новому потужному методу *квадратичного решета*, розробленого Карлом Померанцем в 1981 році. Координація обчислень здійснювалась через Інтернет. Факторизацію RSA-129 було опубліковано в 1994 році

$$\begin{aligned}\text{RSA-129} = {} & 3490529510\ 8476509491\ 4784961990\ 3898133417\ 7646384933 \\ & 8784399082\ 0577 \\ & \times 3276913299\ 3266709549\ 9619881908\ 3446141317\ 76429679 \\ & 929425397\ 98288533.\end{aligned}$$

разом з дешифрованою фразою

```
The magic words are squeamish ossifrage
```

яка не мала особливого смислу: Рівест пояснював, що слова, які формують фразу, було обрано випадковим чином.

Отримані за розв'язанні цієї задачі 100 доларів США були пожертвувані Фонду вільного програмного забезпечення (Free Software Foundation) — некомерційній організації, заснованій Р. Сталлменом у жовтні 1985 року для підтримки руху вільного програмного забезпечення і, особливо, проекту GNU.

3.5. Припущення щодо RSA. Віра в метод RSA базується на трьох припущеннях.

Правило 3. Три припущення щодо RSA

1. Найкращим способом дешифрувати повідомлення є використання приватного ключа.
2. Найкращим способом знайти приватний ключ є обчислення $k^{-1} \pmod{\phi(n)}$.
3. Найкращим способом обчислити $\phi(n)$ є факторизація числа n.

Найменш обгрунтованим здається перше припущення. Існує принаймні два пояснення щодо його доцільності. Перше полягає у тому, що метод грубої сили базується на послідовному переборі всіх чисел i з метою досягти врешті решт значення $k^{-1} \pmod{\phi(n)}$. Для кожного чергового числа i необхідно здійснити дешифрацію повідомлення m, тобто обчислити $x \equiv y^i \pmod{n}$, де y — це шифр повідомлення m, тобто $y \equiv m^k \pmod{n}$. Якщо спроба виявиться безуспішною, то перейти до наступного i. Цей спосіб потребує не менше обчислень, ніж факторизація числа n.

Друга обставина на користь першого припущення, полягає у тому, що якщо оригінальний текст написано іншою мовою, то простий перебір може так і не дати потрібного результату, оскільки результатом дешифрації при кожному i буде незнайомий текст.

3.6. Інший спосіб запису RSA. При використанні методу RSA `Аліса` спочатку виконує алгоритм 1.

Алгоритм 1. RSA: вибір параметрів

1. Обрати два великих простих числа $p \neq q$.
2. Обчислити $n = pq$ та $\phi(n) = (p-1)(q-1)$.
3. Обрати $1 < k < \phi(n)$ так, щоб $(k, \phi(n)) = 1$.
4. Знайти j, для якого $kj \equiv 1 \pmod{\phi(n)}$.
5. Опублікувати n та k.

Знаючи відкритий ключ, `Боб` шифрує своє повідомлення згідно алгоритму 2. необхідно діяти згідно

Алгоритм 2. RSA: шифрування

Вхідні дані: Відкритий ключ (k, n) та повідомлення $m < \min\{p, q\}$;
Вихідні дані: зашифроване повідомлення $y \equiv m^k \pmod{n}$.

`Аліса` дешифрує його повідомлення згідно алгоритму 3.

Алгоритм 3. RSA: дешифрування

Вхідні дані: Відкритий ключ (k, n), приватна експонента j та зашифроване повідомлення y;
Вихідні дані: справжнє повідомлення $m \equiv y^j \pmod{n}$.

Зауваження 2. Бачимо, що алгоритм RSA дозволяє шифрувати тексти з числовим еквівалентом, що не перевищує $\min\{p, q\}$. Це означає, що оригінальний текст попередньо

необхідно розбити на групи, кожна з яких складається не більше, ніж з $\min\{p,q\}-1$ символів. ⑥

4. Доведення алгоритму RSA

Нагадаємо, що $m < \min\{p,q\}$. Нехай $y = m^k \pmod{n}$. Ми знайдемо $y^j \pmod{n}$. За означенням $y = sn + m^k$ для деякого цілого числа s. Тому

$$\begin{aligned} y^j \pmod{n} &= \left(m^k + sn\right)^j \pmod{n} = m^{kj} \pmod{n} \\ &= m^{t(p-1)(q-1)+1} \pmod{n} \end{aligned}$$

для деякого невід'ємного цілого числа t. Остання рівність справджується в силу $kj \equiv 1 \pmod{\phi(n)}$. Таким чином

$$y^j \pmod{n} = m \cdot m^{t(p-1)(q-1)} \pmod{n}. \tag{1}$$

Оскільки $m < p$, то m не ділиться на p. Тому й $m^{t(q-1)}$ не ділиться на p, тобто p та $m^{t(q-1)}$ є взаємно простими. Тепер з малої теореми Ферма (теорема 6.3) випливає

$$\left(m^{t(q-1)}\right)^{p-1} \equiv 1 \pmod{p}$$

й тому

$$m \equiv m \cdot m^{t(p-1)(q-1)} \pmod{p}.$$

Аналогічно доводимо, що

$$\left(m^{t(p-1)}\right)^{q-1} \equiv 1 \pmod{q},$$

[6] Пояснити, чому наведені дії є еквівалентними способу, який ми обговорювали вище?

оскільки $m^{t(p-1)}$ не ділиться на q, звідки

$$m \cdot m^{t(p-1)(q-1)} \equiv m \pmod{q}.$$

За лемою 8.4,

$$m \cdot m^{t(p-1)(q-1)} \equiv m \pmod{pq}. \tag{2}$$

Згадавши, що $n = pq$, з (1) та (2) отримуємо

$$y^j \equiv m \pmod{n}.$$

□

Приклад 1. Розглянемо просту (та нереалістичну) RSA систему шифрування. `Аліса` згідно до алгоритму 1 обирає два простих числа $p = 3$, $q = 5$ й обчислює $n = 15$, $\phi(n) = 8$. Далі вона обирає $k = 3$ й знаходить j, для якого $kj \equiv 1 \pmod{\phi(n)}$, тобто $j = 3$. Нарешті `Аліса` публікує k та n.

`Боб` згідно алгоритму 2 шифрує дуже коротке повідомлення "`Б`", тобто $m = \mathcal{P}_{\texttt{Б}} = 2$:

$$y \equiv m^5 \pmod{n} \equiv 2^5 \pmod{15} = 8.$$

Отримавши повідомлення `Аліса` дешифрує його за допомогою алгоритму 3:

$$x \equiv m^j \pmod{n} \equiv 8^3 \pmod{15} = 2.$$

Таким чином, `Аліса` отримала повідомлення "`Б`".

5. Задача про рюкзак в криптографії

Наступна комбінаторна *задача про рюкзак* має застосування у криптографії. Нехай об'єм рюкзака дорівнює V. Чи можна його заповнити повністю деякими предметами, які мають об'єми $a_1, \dots, a_n$? Іншими словами, чи має задача

$$V = a_1x_1 + a_2x_2 + \cdots + a_na_n \tag{3}$$

розв'язок $x_1, \dots, x_n$, де $x_i = 0$ або $x_i = 1$ для кожного $i = 1, 2, \dots, n$? В залежності від V та $a_1, \dots, a_n$ задача про рюкзак може не мати розв'язків або мати декілька розв'язків.

5.1. Задача про рюкзак для суперзростаючих послідовностей. Існує простий алгоритм знаходження розв'язку задачі про рюкзак (3), якщо $a_1, \dots, a_n$ є *суперзростаючою* послідовністю, тобто такою, що $a_i > a_1 + \cdots + a_{i-1}$ для $2 < i \leq n$. Припустимо, що V дійсно дорівнює сумі деяких чисел a_i, індекси яких утворюють певну множину в $\{1, 2, \dots, n\}$, тобто $V \leq a_1 + \cdots + a_n$.

Якщо $V \geq a_n$, то обов'язково $x_n = 1$, оскільки $a_1 + \cdots + a_{n-1} < a_n \leq V$, тобто в цьому випадку не існує розв'язку з $x_n = 0$. Якщо ж $V < a_n$, то обов'язково $x_n = 0$. Визначивши таким чином x_n, зводимо початкову задачу до іншої задачі про рюкзак

$$V - a_nx_n = a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1}.$$

До цієї задачі застосовуємо аналогічні міркування й через кілька кроків визначимо усі $x_n, x_{n-1}, \dots, x_1$.

5.2. Криптосистема, основана на задачі про рюкзак. В 1978 році Р. Меркл та М. Хеллман запропонували наступну криптографічну систему, основану на задачі про рюкзак. Аліса запроваджує свою систему шифрування, обираючи спочатку деяку суперзростаючу послідовність $a_1, a_2, \ldots, a_n$, модуль $m > 2a_n$ та множник a, $0 < a < m$, для якого $(a, m) = 1$. При такому виборі рівняння $ax \equiv 1 \pmod{m}$ має єдиний розв'язок. Позначимо його через c. Тепер Аліса обчислює

$$b_i \equiv aa_i \pmod{m}, \qquad 1 \leq i \leq n.$$

Зрозуміло, що $0 < b_i < m$, $1 \leq i \leq m$. Послідовність $b_1, \ldots, b_n$, отримана після такого перетворення послідовності $a_1, \ldots, a_n$, як правило, не є суперзростаючою.

Послідовність $a_1, \ldots, a_n$ та числа a та m є приватним ключем Аліси, тоді як послідовність $b_1, \ldots, b_n$ є її відкритим ключем. Кожен, хто бажає надіслати повідомлення Алісі, використовує $b_1, \ldots, b_n$ у якості ключа для шифрування.

Якщо Боб бажає надіслати повідомлення Алісі, то першою його дією є переведення позицій букв у двійкове пред-

ставлення, використовуючи таблицю:

А	1	000001	І	12	001100	Т	23	010111
Б	2	000010	Ї	13	001101	У	24	011000
В	3	000011	Й	14	001110	Ф	25	011001
Г	4	000100	К	15	001111	Х	26	011010
Ґ	5	000101	Л	16	010000	Ц	27	011011
Д	6	000110	М	17	010001	Ч	28	011100
Е	7	000111	Н	18	010010	Ш	29	011101
Є	8	001000	О	19	010011	Щ	30	011110
Ж	9	001001	П	20	010100	Ь	31	011111
З	10	001010	Р	21	010101	Ю	32	100000
И	11	001011	С	22	010110	Я	33	100001

Отриману послідовність `Боб` розбиває на блоки по n бінарних цифр. Останній блок при необхідності доповнюється одиницями. Тепер кожен блок $x_1, \ldots, x_n$ кодується за допомогою відкритого ключа `Аліси` $b_1, \ldots, b_n$:

$$S = b_1x_1 + b_2x_2 + \cdots + b_nx_n.$$

Саме S є шифром блока $x_1, \ldots, x_n$, а послідовність чисел S, які відповідають різним блокам, є шифром повідомлення.

Зрозуміло, що дешифрація блока є рівносильною розв'язанню задачі рюкзака, але не для суперзростаючої послідовності $b_1, \ldots, b_n$. На перший погляд, це ж стосується й `Аліси`, тобто вона не має переваги перед іншими, хоча й саме вона започаткувала цю систему. Насправді ж `Аліса` має перевагу перед іншими. Вона обчислює

$$\begin{aligned} S' &\equiv cS \pmod m \equiv cb_1x_1 + cb_2x_2 + \cdots + cb_nx_n \pmod m \\ &\equiv caa_1x_1 + caa_2x_2 + \cdots + caa_nx_n \pmod m. \end{aligned}$$

Оскільки $ca \equiv 1 \pmod{m}$, то

$$S' \equiv a_1x_1 + a_2x_2 + \cdots + a_nx_n \pmod{m}.$$

Тепер знайти $x_1, \ldots, x_n$ нескладно, оскільки послідовність $a_1, \ldots, a_n$ є суперзростаючою (див. §5.1).

6. Метод Ель-Гамаля

У 1985 році Тахер Ель-Гамаль запрпонував метод шифрування, оснований на одному з варіантів *задачі про дискретні логарифми*. Ця задача полягає у знаходженні показника $0 < x < \phi(n)$, для якого $r^x \equiv y \pmod{n}$ для заданих r, y та n. Показник x *дискретним логарифмом* числа y для основи r по модулю n. Щоб зрозуміти ідею Ель-Гамаля, необхідно знати поняттям *примітивного кореня*.

6.1. Примітивний корінь числа. Число a називається примітивним коренем для $n > 1$, якщо

(i) $(a, n) = 1$;
(ii) $a^k \not\equiv 1 \pmod{n}$ для будь-якого $0 < k < \phi(n)$.

Зауважимо, що $a^{\phi(n)} \equiv 1 \pmod{n}$ за теоремою Ойлера (теорема 6.2).

Приклад 2. Щоб довести, що 3 є примітивним коренем для 7, зауважимо, що $\phi(7) = 6$ та

k	1	2	3	4	5	6
3^k	3	9	27	81	243	729
$3^k \pmod{7}$	3	2	6	4	5	1

Можна довести, що примітивний корінь існує для будь-якого простого числа. Примітивні корені існують також і

для деяких непростих чисел, хоча і не для всіх. Існування примітивного кореня для натурального числа є скоріше виключенням. Наприклад, число mn не має примітивного кореня, якщо $m > 2$, $n > 2$ та $(m, n) = 1$. Більше того, тільки числа 2, 4, p^k та $2p^k$ мають примітивні корені, де p — просте число, а k — натуральне.

Нижче наведено таблицю примітивних коренів χ_p для перших простих чисел p:

Таблиця 1
Примітивні корені χ_p для перших простих чисел p

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
χ_p	1	2	2	3	2	2	3	2	5	2	3	2	6	3	5	2	2	2	2	7

6.2. Криптосистема Ель-Гамаля. Щоб заснувати свою криптосистему, `Аліса` спочатку обирає параметри, як описано у наступному алгоритмі.

Алгоритм 4. Метод Ель-Гамаля: вибір параметрів

1. Обрати просте число p
2. Обчислити примітивний корінь r для p
3. Випадковим чином вибрати k, $2 \le k \le p - 2$
4. Обчислити $a \equiv r^k \pmod{p}$

Відкритим ключем `Аліси` є трійка (p, r, a). Число k є її приватним ключем.

`Боб` переводить своє повідомлення у цифровий формат й використовує відкритий ключ `Аліси`, щоб надіслати їй повідомлення, використовуючи наступний алгоритм.

Алгоритм 5. Метод Ель-Гамаля: шифрування

Вхідні дані: Відкритий ключ Аліси (p, r, a); повідомлення m

Вихідні дані: Зашифроване повідомлення

1. Розбити послідовність десяткових цифр m на блоки $B < p$.
2. Випадковим чином обирає натуральне число j, $2 \le j \le p-2$.
3. Для кожного блоку B обчислює $C_1 \equiv r^j \pmod{p}$ та
   $C_2 \equiv Ba^j \pmod{p}$.
4. Шифром повідомлення є послідовність пар (C_1, C_2).

Зауважимо, що число j може змінюватись з кожним наступним блоком. Це надасть ще більшої стійкості методу шифрування Ель-Гамаля.

Отримавши повідомлення від Боба, яке складається з m пар $(C_1^{(i)}, C_2^{(i)})$, $1 \le i \le m$, Аліса використовує свій приватний ключ k й дешифрує кожний блок за допомогою наступного алгоритму.

Алгоритм 6. Метод Ель-Гамаля: дешифрування

Вхідні дані: Відкритий ключ (p, r, a) та приватний ключ k;
зашифроване повідомлення $(C_1^{(i)}, C_2^{(i)})$, $1 \le i \le m$.

Вихідні дані: Дешифроване повідомлення

1. Для кожної пари (C_1, C_2) обчислити
   $C_1^{p-k-1} \pmod{p}$ й потім
   $T \equiv C_2 C_1^{k-p-1} \pmod{p}$.
2. Дешифрованим повідомленням є послідовність чисел T.

Щоб впевнитись, що Аліса правильно дешифрує повідомлення Боба, зауважимо, що

$$\begin{aligned} T &\equiv C_2 C_1^{p-k-1} \pmod{p} \equiv (Ba^j) \cdot (r^j)^{p-k-1} \pmod{p} \\ &\equiv B(r^k)^j \cdot r^{j(p-1)-jk} \pmod{p} \\ &\equiv B(r^{p-1})^j \pmod{p} \equiv B \pmod{p}. \end{aligned}$$

Остання конгруенція є справедливою на підставі малої теореми Ферма (теорема 6.3). ⑦

Приклад 3. Припустимо, що відкритим ключем Аліси є трійка $(p, r, a) = (43, 3, 22)$, а приватним — число $k = 15$. Згідно до алгоритму 4 вибору параметрів шифру, необхідно $a \equiv r^k \pmod{p}$, тобто $22 \equiv 3^{15} \pmod{43}$. ⑧

Припустимо далі, що Боб хоче надіслати повідомлення "НОВИЙ". Перш за все він переводить його у цифровий формат: НОВИЙ=1819031114. Наступним кроком Боб розбиває повідомлення на блоки з двох символів:

НОВИЙ=18 19 03 11 14.

Тепер він обирає $j = 23$. Для спрощення ми вважаємо, що це число є однаковим для всіх блоків. Далі,

$$\begin{aligned} C_1 &\equiv r^j \pmod{p} = 3^{23} \pmod{43} = 34, \\ a^j &\pmod{p} = 22^{23} \pmod{43} = 32. \end{aligned}$$

[7] Перевірити застосування малої теореми Ферма.
[8] Перевірити це.

Після цього Боб обчислює $Ba^j \pmod{p}$ для кожного двосимвольного блоку B. Наприклад, для першого блоку його обчислення є такими

$$C_2 = 18 \cdot 32 \equiv 17 \pmod{43}.$$

Таким чином, шифром першого блоку є пара $(34, 17)$. Для інших блоків обчислення цілком аналогічні.

Отримавши повідомлення, Аліса діє згідно до алгоритму 6:

$$C_1^{p-k-1} \pmod{p} = 34^{43-15-1} \pmod{43} = 34^{27} \pmod{43} = 39.$$

⑨ Подальші обчислення для відтворення першого символу є такими:

$$T \equiv C_2 C_1^{p-k-1} \pmod{p} = 17 \cdot 39 \pmod{43} = 18.$$

⑩ Аліса правильно дешифрувала перший символ повідомлення Боба.

7. Контрольні питання

1. Перевірте ще раз! (стор. 220).

2. Пригадайте, чому $\phi(n) = (p-1)(q-1)$? (стор. 221).

3. Пригадайте, чому ця властивість є вірною? (стор. 221).

4. Пояснити, чому не обов'язково вимагати, щоб k було дуже великим числом? (стор. 221).

5. Чи дійсно знання j є еквівалентним до знання (p, q)? (стор. 222).

6. Пояснити, чому наведені дії є еквівалентними способу, який ми обговорювали вище? (стор. 226).

[9] Впевнитись, що $34^{27} \pmod{43} = 39$.

[10] Впевнитись, що $17 \cdot 39 \pmod{43} = 18$.

7. Перевірити застосування малої теореми Ферма. (стор. 235).
8. Перевірити це. (стор. 235).
9. Впевнитись, що $34^{27} \pmod{43} = 39$. (стор. 236).
10. Впевнитись, що $17 \cdot 39 \pmod{43} = 18$. (стор. 236).

8. Задачі

Задача 1. *Використовуючи відкритий ключ RSA криптосистеми* $(n, k) = (2773, 21)$ *зашифрувати повідомлення*

SILENCE IS GOLD

Задача 2. *Нехай* $n = pq$, *де* p *та* q — *прості числа. Довести, що* $p + q = n - \phi(n) + 1$.

Задача 3. *Нехай* $n = pq$, *де* p *та* q — *прості числа. Довести, що* $|p - q| = \sqrt{(p+q)^2 - 4n}$.

Задача 4. *Нехай* $n = pq$, *де* p *та* q — *прості числа. Виразити* p *та* q *через* n.

Задача 5. *Відомо, що в криптосистемі RSA* $n = pq = 274279$ *та* $\phi(n) = 272376$. *Знайти* p *та* q.

Задача 6. *Припустимо, що відкритим ключем криптосистеми RSA є* $(n, k) = (3233, 37)$. *Визначити приватний ключ.*

Задача 7. *За допомогою RSA алгоритму з відкритим ключем* $(n, k) = 1643, 223)$ *отримано шифроване повідомлення*

0833 0823 1130 0055 0329 1099

Дешифрувати повідомлення, написане англійською мовою.

Задача 8. *Припустимо, що криптоаналітик аналізує повідомлення* M, *яке було зашифровано за допомогою методу RSA. Виявилось, що* M *не є взаємно простим з* $n = pq$, *де* p *та* q *є простими числами. Показати, що в цьому випадку факторизація* n *є простою задачею.*

Задача 9. *Припустимо, що* Боб *обрав* n, $n = pq$, *для своєї RSA криптосистеми, де* p *and* q *два великих простих числа, та два показника* k_1 *та* k_2. *Він просить* Алісу *шифрувати повідомлення, які вона надсилає, спочатку RSA шифром з ключем* (n, k_1), *а потім ще раз з ключем* (n, k_2). *Чи додає такий спосіб шифрування більшої безпеки у листуванні між* Алісою *та* Бобом*?*

Задача 10. *Припустимо, що у своїх RSA криптосистемах* Аліса *та* Боб *використовують спільний модуль* n, *але різні показники* k_1 *та* k_2. *Припустимо, що* Аліса *надсилає* Бобу *повідомлення* M, *зашифроване його відкритим ключем* (n, k_2), *а* Боб *надсилає* Алісі *те ж саме повідомлення* M, *але зашифроване відкритим ключем* Алісси (n, k_1). *Покажіть, что в цьому випадку відновлення* M *є доволі простою задачею.*

Задача 11. *Припустимо, що система RSA використовується для шифрації повідомлень* M_1 *та* M_2, *а також їхнього добутку* $M = M_1 M_2$. *Показати, що шифр для* M *дорівнює добутку шифрів для* M_1 *та* M_2 *за модулем* n.

Задача 12. *Нехай* $n = 1,342,127$. *Позначимо через* x *найменше з цілих чисел* i, *для яких* $x^2 - n \geq 0$. *Оскільки* $x = 1159$, *то* $\sqrt{x^2 - n}$ *не є цілим, тому збільшимо* x *на одиницю й продовжимо цей процес доти, поки число* $\sqrt{x^2 - n}$ *не стане цілим або не досягнемо межі* $x = (n + 1)/2$. *Обчислення наведено у наступній таблиці:*

x	1159	1160	1161	1162	1163	1164
$\sqrt{x^2 - n}$	33,97	58,93	76,11	90,09	102,18	113

Тому $1,342,127 = 1164 \times 113$. *Перевірити всі наведені обчислення.*

Задача 13. *Розглянемо наступний алгоритм, який носить ім'я Ферма:*

Алгоритм 7. Алгоритм Ферма

Вхідні дані: непарне число n;

Вихідні дані: цілі числа x та y, для яких $n = x^2 - y^2$, або інформація, що n просте.

`Крок 1.` Покладемо $x = \lceil \sqrt{n} \rceil$;
якщо $x^2 = n$, то $y = 0$; STOP
якщо ж $x^2 \neq n$, то збільшити x на одиницю;

`Крок 2.` якщо $x = (n+1)/2$, то n просте; STOP
якщо ж $x < (n+1)/2$, то обчислити $y = \sqrt{x^2 - n}$;

`Крок 3.` якщо y ціле, то $n = (x-y)(x+y)$; STOP
якщо ж y неціле, то збільшити x на одиницю;
перейти до `Кроку 2`;

Довести, що алгоритм 7 є правильним, тобто

a) *якщо n є складеним, то існує натуральне $\sqrt{n} \leq x < (n+1)/2$, для якого $\sqrt{x^2 - n}$ є натуральним числом*;
b) *якщо n є простим, то $\sqrt{x^2 - n}$ не є натуральним числом для будь-якого $x < (n+1)/2$.*

Задача 14. *Зазначимо, що у загальному випадку кожне натуральне число n можна представити у вигляді $n = ab$ для $1 < a < b < n$ кількома різними способами. Яке ж з таких представлень знаходить алгоритм 7?*

Задача 15. *Довести, що алгоритм 7 ніколи не закінчиться, якщо $n = 2k$ для непарного числа k.*

Задача 16. *Розглянемо такий цифровий алфавіт на базі латинсь-*

кого:

A=00	K=10	U=20	1=30	
B=01	L=11	V=21	2=31	
C=02	M=12	W=22	3=32	
D=03	N=13	X=23	4=33	
E=04	O=14	Y=24	5=34	
F=05	P=15	Z=25	6=35	
G=06	Q=16	,=26	7=36	
H=07	R=17	.=27	8=37	
I=08	S=18	?=28	9=38	
J=09	T=19	0=29	!=39	$\sqcup$ = 99

a) *Записати фразу* `NO WAY` *у цьому цифровому алфавіті.*
b) *Оберемо* $k = 47$, $p = 29$, $q = 53$. *Чи можна користуватись таким шифром* $RSA_{k,p\cdot q}$*?*
c) *Позначимо цифровий запис фрази з* a) *через* M. *Десяткові цифри в* M *об'єднаємо у групи по три. Зашифрувати кожну з груп за допомогою шифра* $RSA_{k,p\cdot q}$, *де числа* k, p *та* q *визначені в* b).
d) *Визначити експоненту* j *для дешифрації шифру* $RSA_{47,29\cdot 53}$. *Дешифрувати повідомлення, яке отримано в* c). *Перевести його у звичайний формат.*

Задача 17. *Довести, що задача про рюкзак*

a) $22 = 3x_1 + 7x_2 + 9x_3 + 11x_4 + 20x_5$ *не має розв'язків*;
a) $27 = 3x_1 + 7x_2 + 9x_3 + 11x_4 + 20x_5$ *має декілька розв'язків.*

Задача 18. *Нехай* $a_i = 2^i$ *для всіх* $0 \le i \le n$, *а* $V < 2^{n+1}$. *Довести, що задача про рюкзак має єдиний розв'язок.*

Задача 19. *Знайти розв'язок наступної задачі про рюкзак*

$$28 = 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5.$$

Задача 20. a) *Впевнитись, що алгоритм у §5.1 дійсно знаходить розв'язок початкової задачі.*

b) *Довести, що цей розв'язок є єдиним.*

c) *Перевірити, що послідовності* $a_1, \ldots, a_n$ *в задачах* 18 *та* 19 *є суперзростаючими.*

Задача 21. a) *Використовуючи суперзростаючу послідовність* $a_1 = 1$, $a_2 = 2$, $a_3 = 4$, *модуль* $m = 9$ *та множник* $a = 4$, *обчислити послідовність* b_1, b_2, b_3.

b) *Перевести в бінарну систему повідомлення* ПРИВІТ.

c) *Зашифрувати повідомлення* ПРИВІТ, *використовуючи криптосистему, основану на задачі про рюкзак та відкритий ключ* b_1, b_2, b_3, *обчислений у* a).

d) *Перевірити алгоритм дешифрації на результаті, отриманому в* c).

Задача 22. Аліса *створює свою криптосистему, обираючи суперзростаючу послідовність* $a_1 = 3$, $a_2 = 5$, $a_3 = 11$, $a_4 = 20$, $a_5 = 41$, *а також модуль* $m = 85$ *та множник* $a = 44$.

a) *Обчислити відкритий ключ* b_1, b_2, b_3, b_4, b_5 *криптосистеми* Аліси.

b) *Знайти* c, *для якого* $44c \equiv 1 \pmod{85}$.

Боб *хоче передати* Алісі *повідомлення* HELP US.

c) *Використовуючи цифровий алфавіт з задачі* 16, *перевести це повідомлення у бінарний формат.*

d) *Зашифрувати повідомлення* Боба *за допомогою відкритого ключа.*

Щоб дешифрувати повідомлення Боба, Аліса *спочатку обчислює код повідомлення* Боба *для її суперзростаючої послідовності, а потім розв'язує задачу про рюкзак для кожного блока.*

e) *Перекодувати повідомлення* Боба *для приватного коду* Аліси.

f) *Дешифрувати повідомлення* Боба.

Задача 23. *Знайти всі розвязки задачі про рюкзак*

$$21 = 2x_1 + 3x_2 + 5x_3 + 7x_4 + 9x_5 + 11x_6.$$

Задача 24. *Які з послідовностей, наведених нижче, є суперзростаючими:*

a) 3, 13, 20, 37, 81.
b) 5, 13, 25, 42, 90.
c) 7, 27, 47, 97, 197, 397.

Задача 25. *Знайти єдиний розвязок кожної з наступних задач про рюкзак з суперзростаючою послідовністю:*

a) $118 = 4x_1 + 5x_2 + 10x_3 + 20x_4 + 41x_5 + 99x_6$.
b) $51 = 3x_1 + 5x_2 + 9x_3 + 18x_4 + 37x_5$.
c) $54 = x_1 + 2x_2 + 5x_3 + 9x_4 + 18x_5 + 40x_6$.

Задача 26. *Нехай послідовність доатних цілих чисел $a_1, a_2, \ldots, a_n$ має властивість $a_{i+1} > 2a_i$ для всіх $i = 1, 2, \ldots, n-1$. Довести, що ця послідовність є суперзростаючою.*

Задача 27. *Відкритим ключем рюкзачної криптосистеми є* 49, 32, 30, 43. *Якщо приватний модуль дорівнює $m = 50$, а множник — $a = 33$, то якою є приватна суперзростаюча послідовність*?

Задача 28. `Аліса` *використовує у своїй рюкзачній криптосистемі суперзростаючу послідовність* 1, 3, 5, 11, 35, *модуль $m = 73$ та множник $a = 5$.* `Боб` *надіслав* `Алісі` *повідомлення* `55, 15, 124, 109, 25, 34`. *Що написав* `Боб`?

Задача 29. *Приватним ключем рюкзачної криптосистеми* `Аліси` *є суперзростаюча послідовність* 2, 3, 7, 13, 27, *модуль $m = 60$ та множник $a = 1$.*

a) *Знайти відкритий ключ цієї криптосистеми.*
b) *За допомогою відкритого ключа зашифрувати повідомлення* `SEND MONEY`.

Задача 30. *Закінчити обчислення для інших блоків у прикладі 3.*

Задача 31. *Криптосистема Ель-Гамаля має приватний ключ $k = 30$ та відкритий ключ $(p, r, a) = (71, 7, 32)$. Дешифрувати повідомлення*

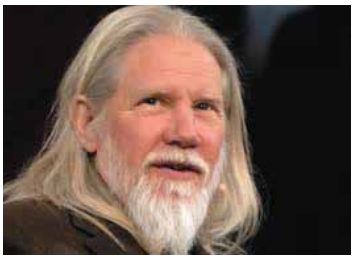
$$\begin{array}{ccccc} (56,45) & (56,38) & (56,29) & (56,03) & (56,67) \\ (56,05) & (56,27) & (56,31) & (56,38) & (56,29) \end{array}$$

яке написано англійською мовою.

Задача 32. *Криптосистема Ель-Гамаля має приватний ключ* $k = 17$ *та відкритий ключ* $(p, r, a) = (37, 2, 18)$. `Боб` *надсилає повідомлення* "`NOT NOW`", *використовуючи в циклі* $j = 13$, $j = 28$ *та* $j = 11$.

a) *Яким є зашифроване повідомлення* `Боба`?
b) *Як* `Аліса` *відтворює це повідомлення*?

БІОГРАФІЇ



Діффі, *Вітфілд* (нар. 5.06.1944), американський криптограф, один з найвідоміших спеціалістів, що заслужив світову популярність за концепцію криптографії з відкритим ключем. Його інтерес до криптографії з'явився у віці 10 років, коли батько (професор, викладав іспанську історію та культуру) приніс додому книги з криптографії. У 1965 році Діффі отримав ступінь бакалавра в Массачусетському технологічному інституті. В 1974 році Діффі познайомився з Мартіном Хеллманом, професором факультету електротехніки Стенфордського університету (див. [Хеллман], стор. 195). У спільній роботі, яку було опубліковано в 1976 році, вони розглянули революційно новий метод, якій пізніше стали називати системою обміну ключами Діффі–Хеллмана.

В Стенфордському університеті
М. Хеллман (у центрі) та В. Діффі (праворуч)

Діффі вважається одним з перших *шіфропанків* — людей, які вважають що приватна інформація є недоторканною і повинна бути захищена за допомогою криптографії. Він є затятим противником спроб уряду обмежити використання криптографії в персональних цілях і багато разів виступав у сенаті США, захищаючи свою позицію.

Еделман, *Леонард* (нар. 31.12.1945), американський учений-теоретик у галузі комп'ютерних наук. Він відомий як співавтор системи шифрування RSA і принципів ДНК-обчислень. Отримав ступінь бакалавра з математики у 1968 році в університеті Берклі. Леонард Еделман, разом з Рональдом Рівестом (див. [Рівест], стор. 247) та Аді Шаміром (див. [Шамір], стор. 249), отримав премію Тьюринга 2002 року (яку часто називають Нобелівською премією у галузі комп'ютерних наук) за внесок у винахід криптосистеми RSA.

Л. Еделман відомий своїм терміном *комп'ютерний вірус*. Він вважає, що комп'ютерні віруси відкривають багато можливостей в технологіях майбутнього і що користь, отримана від них, потенційно може переважити негативні сторони їх використання.

В останні роки він розробляє застосування ДНК у якості обчислювальної системи.

> *Найголовніше в ДНК-обчисленнях є те, що вони показують, що молекули ДНК можуть зробити таке, що зазвичай вважається можливим лише для комп'ютерів. Це означає, що комп'ютерна наука і біологія тісно пов'язані. Кожну живу істоту можна розглядати, як обчислювальну систему, і інколи живі істоти можна зрозуміти краще, якщо дивитись на них їх, як на комп'ютери.*
>
> Л. Еделман

В результаті робіт Еделмана у галузі молекулярної біології було створено математичну модель імунної недостатності, викликаної вірусом СНІД. Це дало розуміння того, як вірус працює, а також відкрило різні напрями досліджень для пошуку шляхів лікування. Л. Еделман та Д. Вофсі описали результати перевірки однієї з гіпотез про розвиток синдрому набутого імунного дефіциту.

Проте Л. Еделман найбільше пишається своєю роботою (спільною з К. Померанцем (див. [Померанц], стор. 247) та Р. Румлі) про новий метод перевірки чисел на простоту (опубліковано в 1983 році). Цей

метод дозволяє перевірити простоту числа n за час $O\left((\ln n)^{c \ln\ln\ln n}\right)$, c — деяка універсальна константа.

Ель-Гамаль, *Тахер* (нар. 18.08.1955), єгипетський криптограф, створив численні технології та стандарти для безпечного використання даних та цифрових підписів. Він є автором криптосистеми, основаній на задачі про дискретний логарифм. Його система цифрового підпису використана при розробці широко відомого алгоритму DSA (*Digital Signature Algorithm*), який пізніше став стандартом DSS (*Digital Signature Standard*) в США. Ель-Гамаль не зміг запатентувати свій алгоритм, оскільки був іноземним випускником Стенфордського університету. Згідно закону він повинен був залишатися студентом до моменту видачі патенту. Ель-Гамаль вирішив опублікувати свої дослідження, які стали надбанням громадськості. Завдяки такому кроку його ім'я стало відомим в усьому світі.

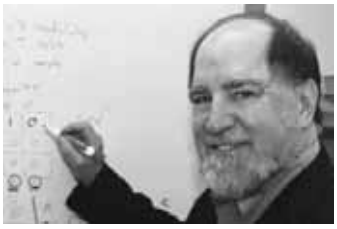
Він приймав участь у розробці платіжного протоколу SET для кредитних карток, а також ряду платіжних систем для Інтернету. Його називають "батьком SSL" — протоколу безпечного з'єднання в Інтернеті. Керівником його магістерської дисертації в Стенфордському університеті був М. Хеллман (див. [Хеллман], стор. 195).

Меркл, *Ральф* (нар. 2.02.1952), американський криптограф, відомий своїми роботами у галузі криптографічних систем з відкритими ключами (протокол Діффі–Хеллмана–Меркла) і хешування (так звана структура Меркла–Дамгарда). В 1974 році отримав в університеті Берклі ступінь бакалавра у галузі інформатики. Починаючи з 1975 року, Меркл цікавився методами захисту ліній передачі даних. Використовуючи ідею змішування випадкових чисел, він намагався розв'язати проблему обміну відкритими ключами.

Після зустрічі з М. Хеллманом (див. [Хеллман], стор. 195), Меркл продовжив аспірантуру в Стенфордському університеті. За допомогою Хеллмана і Діффі (див. [Діффі], стор. 244) у 1976 році він зміг досягти успіху у розробці теорії цифрового підпису.

В останні роки Меркл намагається довести реальність ідеї *кріоніки* (наука про збереження в стані глибокого охолодження людей і тварин в надії на те, що в майбутньому їх вдасться оживити і при необхідності — вилікувати). Є директором *Alcor*'а — некомерційної організації, яка займається *кріонікою*.

Померанц, *Карл* (нар. у 1944 р.), американський математик та криптограф, фахівець з теорії чисел. Ступінь магістра отримав в Гарвардському університеті. У кандидатській дисертації довів, що кожне досконале число має принаймні 7 простих дільників. Він є автором одного з найбільш важливих алгоритмів факторизації цілих чисел — методу квадратичного решета, за допомогою якого в 1994 році вдалося зламати RSA–129. Він є одним з авторів алгоритму Еделмана–Померанца–Румлі для перевірки чисел на простоту (див. [Едельман], стор. 244). Він є автором понад 200 публікацій, у тому числі основоположної книги "*Прості числа: Криптографічні та обчислювальні аспекти*" (разом з Р. Крендаллом).



Рівест, *Роналд* (нар. 7.05.1947), американський спеціаліст з криптографії. Має ступінь бакалавра з математики від Єльського університету (1969 рік) та вчений ступінь доктора філософії з комп'ютерних наук від Стенфордського університету (1974 рік). Він є одним з авторів криптографічного алгоритму RSA разом з Аді Шаміром (див. [Шамір], стор. 249) і Леонардом Еделманом (див. [Еделман], стор. 244). Ідея алгоритму осінила його в ніч на свято єврейської Пасхи, у якій брала участь

вся трійця алгоритму RSA. Але ця ідея визріла після довгих спільних досліджень протягом року.

Автори RSA
зліва направо: А. Шамір, Р. Рівест, Л. Еделман

Спільно з Еделманом і Шаміром, Рівест заснував компанію для випуску RSA-чіпів. Еделман був президентом компанії, Рівест — головою правління, а Шамір — скарбником. В 1983 році компанію придбала корпорація "*Security dynamics*".

Рівест є автором таки алгоритмів симетричного шифрування як RC2, RC4, RC5; він також брав участь в розробці RC6. Шифри RC1 та RC3 виявились вразливими. Взагалі, літери *RC* означають *Rivest Cipher* (шифр Рівеста).

У 2006 році Рівест разом з У. Смітом опублікував ідею системи голосування "*ThreeBallot*", яка дозволяє виборцю упевнитися у тому, що його голос врахований на виборах при збереженні повної конфіденційності. Цікаво, що ця система жодним чином не використовує криптографію. Більше того, ця система не використовує компьютери; для її функціонування потрібні лише технологічно прості пристрої для голосування. Голосування є таємним, але перевіряється самим виборцем. Рівест опублікував систему як суспільне надбання, під девізом "*Наша демократія є надто важливою для нас*".

Сталлмен, *Річард* (нар. 16.03.1953), засновник руху вільного програмного забезпечення, а також проекту GNU, Фонду вільних програм та Ліги за свободу програмування. Автор концепції, втіленої у ліцензії GNU General Public License (GNU GPL) для комп'ютерних програм. Столмен радить не користуватися мобільними телефонами, тому, що вважає, що можливість визначення місцезнаходження телефону може створити різні проблеми для абонента.

Шамір, *Аді* (нар. 6.07.1952), відомий ізраїльський криптоаналітик, вчений у галузі теорії обчислювальних систем, професор прикладної математики в інституті Вейцмана, лауреат премії Тьюринга за "... *унікальний внесок у збільшення практичної цінності систем шифрування* ... ". Спільно з Роналдом Рівестом (див. [Рівест], стор. 247) і Леонардом Еделманом (див. [Еделман], стор. 244) розробив знамениту криптосхему з відкритим ключем RSA. А. Шамір отримав ступінь бакалавра від Тель-Авівського університету (1973), магістра (1975) і доктора філософії з інформатики (1977) від інституту Вейцмана. Крім RSA, Аді Шамір відомий розробкою (1979) схеми "розподіленого" секрету, математичного методу для розподілу деякого "секрету" серед кількох "учасників" з можливістю подальшої його реконструкції. У 1986 році він брав участь у розробці протоколу аутентифікації, названого згодом протоколом Фейга–Фіата–Шаміра. Шамір разом зі своїм учнем Е. Біхамом розробив диференціальний криптоаналіз, метод атаки на блочні шифри.