Лекція 9

КРИПТОАНАЛІЗ ЕКСПОНЕНЦІАЛЬНИХ ШИФРІВ

Дешифрування повідомлення, до якого застосовано експоненціальний шифр, є складною обчислювальною задачею, хоча з точки зору теорії для цього не існує жодних перешкод. Ми розглянемо це питання на прикладах, з яких стане зрозумілим це твердження.

1. Дешифрування у випадку коли степінь та модуль відомі

Розглянемо приклад дешифрування повідомлення, закодованного за допомогою експоненціального шифру з відомими показником та модулем.

Приклад 1. Дешифрувати повідомлення

(1) `4149 3569 4142 2290 1930 4679`

яке було зашифровано за допомогою $E_{k,n}$ шифру з показником $k = 1649$ та модулем $n = 5251$.

Перш за все розкладемо модуль на множники: $5251 = 59 \cdot 89$. Зауважимо, що 59 та 89 є простими числами. Тому з властивості 3 функції Ойлера (див. лекцію 6) випливає, що $\phi(5251) = 58 \cdot 88 = 5104$.

Згідно до формули (8.6), дешифрування здійснюється наступним чином

$$\mathcal{P}_{\mathtt{X}} \equiv \mathcal{C}_{\mathtt{X}}^{j} \pmod{5251},$$

де j — це показник кореня k-ого степеня за модулем n. Згідно правилу 2, наведеному у лекції 8, $j = 1649^{-1} \pmod{5104}$.

Обернене число за модулем знаходимо за допомогою узагальненого алгоритму Евкліда (див. алгоритм 3 у лекції 4):

$$5104 = 1649 \cdot 3 + 157,$$
$$1649 = 157 \cdot 10 + 79,$$
$$157 = 79 \cdot 1 + 78,$$
$$78 = 78 \cdot 1 + 0.$$

Тому таблиця (4.11) має вигляд

		1	1	10	3
0	1	1	2	21	65

Утворюємо лінійну комбінацію

$$1649 \cdot 65 - 5104 \cdot 21 = 1,$$

звідки отримуємо $65 = 1649^{-1} \pmod{5104}$.

Тепер для окремих груп повідомлення (1) обчислюємо остачі від ділення степенів на модуль:

$$4149^{65} \pmod{5251} = 322,$$
$$3569^{65} \pmod{5251} = 702,$$
$$4142^{65} \pmod{5251} = 2406,$$
$$2290^{65} \pmod{5251} = 706,$$
$$1930^{65} \pmod{5251} = 1902,$$
$$4679^{65} \pmod{5251} = 2107.$$

Всі обчислені остачі перевищують 33, тому природно зробити припущення, що спочатку текст було розбито на групи і потім шифрувались групи. Оскільки $33^2 < k < 33^3$ ①, то робимо висновок, що групи складались з двох букв. ②

Тепер переводимо розшифрований цифровий формат в групи з двох букв:

0322	0702	2406	0706	1902	2107
ВС	ЕБ	УД	ЕД	ОБ	РЕ

Нарешті нескладно здогадатись, що зашифровано було наступний текст

(2) ВСЕ БУДЕ ДОБРЕ

Зауваження 1. Зверніть увагу, що число 322 відповідає саме групі ВС, а не ЮБ. ③

Приклад 2. На останньому кроці дешифрування у прикладі 1 було розв'язано "шараду" для отримання тексту (2). Якби при групуванні між словами використовувались символи ␣ (які мають код 00), то цей крок був би непотрібний. Не пояснюючи деталей, покажемо процеси шифрування та дешифрування у цьому випадку. Шифрування здійснюється за формулою

$$\mathcal{C}_{\mathtt{XY}} = (\mathcal{P}_{\mathtt{XY}})^{1649} \pmod{5251}.$$

В наступній таблиці наведено результати шифрування.

Процес шифрування

групи	ВС	Е␣	БУ	ДЕ	␣Д	ОБ	РЕ
$\mathcal{P}_{\mathtt{XY}}$	0322	0700	0224	0607	0006	1902	2107
$\mathcal{C}_{\mathtt{XY}}$	4149	1501	3033	3699	1092	1930	4679

Перша та остання групи у новому тексті такі ж, як і у тексті з прикладу 1, тому їхні шифри також однакові.

Як і у прикладі 1, дешифрування повідомлення з пробілами між словами здійснюється за формулою

$$\mathcal{P}_{\mathtt{XY}} = (\mathcal{C}_{\mathtt{XY}})^{65} \pmod{5251}.$$

В наступній таблиці наведено результати дешифрування.

Процес дешифрування

$\mathcal{C}_{\mathtt{XY}}$	4149	1501	3033	3699	1092	1930	4679
$\mathcal{P}_{\mathtt{XY}}$	322	7	224	67	6	192	217
з нулями	0322	0700	0224	0607	0006	1902	2107
групи	ВС	Е␣	БУ	ДЕ	␣Д	ОБ	РЕ

Зверніть увагу на особливість кодування символа ␣ у різних блоках:

$$\mathtt{E}\text{␣} \to 0700, \qquad \text{␣}\mathtt{Д} \to 0006.$$

Це пояснюється тим, що у першому випадку група Е␣=0700 закінчується символом ␣, а у другому — група ␣Д=0006, з нього починається.

2. Дешифрування у випадку коли показник або модуль невідомі

Дешифрування повідомлення, до якого застосовано експоненціальний шифр з невідомими показником та модулем, майже неможлива без удачі. Розглянемо наступний приклад.

Приклад 3. Дешифрувати повідомлення

```
496 343 0 663 1 94 664 161 664
```

яке було зашифровано за допомогою $E_{k,n}$ шифру.

Аналіз почнемо з аналізу послідовності чисел у шифрованому тексті. Оскільки максимальним числом є `664`, то робимо висновок, що модуль n не є меншим за 665. ④ Числа $665 = 5 \cdot 7 \cdot 19$ та $666 = 2 \cdot 3^2 \cdot 37$ не є простими, а їхній канонічний розклад не має вигляду pq для різних простих чисел p та q. ⑤ Цю властивість має наступне число $667 = 23 \cdot 29$. ⑥ Приймаємо гіпотезу про те, що $n = 667$, хоча не виключено, що ця гіпотеза є помилковою. ⑦

Щоб дешифрувати повідомлення `Аліси`, необхідно перевірити всі степені $k \leq n$, які є взаємно простими з $\phi(n)$ ⑧. Оскільки $\phi(667) = 616$, то таких чисел існує рівно $\phi(616) = \phi\left(2^3 \cdot 7 \cdot 11\right) = 240$. ⑨

Процес дешифрування почнемо з $k = 3$. Знаходимо ⑩

$$3^{-1} \pmod{667} = 411,$$

тому пробне дешифрування здійснюємо за правилом

$$\mathcal{P}_{\mathtt{X}} = (\mathcal{C}_{\mathtt{X}})^{411} \pmod{667}.$$

Результатом дешифрування є ⑪

```
НЕ␣ПАЛИТИ
```

Зауваження 2. Нам пощастило при аналізі шифртексту в прикладі 3, оскільки там зустрілось число 664 й ми зробили

правильне припущення $n = 667$. Крім того, нам не знадобилось перевіряти усі 240 варіантів для показника шифру, оскільки ми вгадали, що $k = 3$. ⑫ Якби припущення $n = 667$ виявилось хибним, то перевірка усіх 240 варіантів для k була б марною, а її результатом стало б те, що всі обчислення необхідно було б повторити, але тепер для $n = 669$. ⑬ Без комп'ютера ці обчислення потребують надто багато часу. Але чи завжди комп'ютер розв'яже задачу?

Приклад 4. Дешифрувати повідомлення

7940 6667 6104 6334 6657 2266 256 6667 1 6460 3662
7815 2147 2401 6334 6667 2266 3757 6657 2266

яке було зашифровано за допомогою $E_{k,n}$ шифру з модулем $n = 8537$.

На перший погляд задача здається простішою, ніж у прикладі 3, оскільки тепер ми знаємо модуль n. Для того, щоб дешифрувати повідомлення, необхідно

(i) знайти всі числа k, взаємно прості з $\phi(n)$;
(ii) для кожного з них визначити j, обернене число за модулем $\phi(n)$;
(iii) для кожного k здійснити пробне $E_{j,n}$ дешифрування.

Перше питання, яке постає при реалізації цієї програми, стосується факторизації числа $n = 8537$. Чи є воно простим? Якщо ні, то які дільники воно має? За допомогою комп'ютера можна встановити, що число $n = 8537$ є простим, тому у найгіршому випадку необхідно перевірити 8536 показників. ⑭

Тепер починаймо перевіряти показники крок за кроком, починаючи з $k = 2$. А чи існує кращий метод? ⑮

Приклад 5. Дешифрувати повідомлення

```
5330549  5278727  9659311  866598  3106889  676181  2027066
```

яке було зашифровано за допомогою $E_{k,n}$ шифру з показником $k = 3$ та модулем $n = 15,002,557$.

Задача є схожею до прикладу 1. Число n має факторизацію $15,002,557 = 2447 \cdot 6131$, ⑯ тому $\phi(n) = 14,993,980$. ⑰ Можна також знайти, що $3^{-1} \pmod{14993980} = 9,995,987$. ⑱ Тепер для дешифрування необхідно для кожного слова в шифрованому повідомленні виконати операцію ⑲

$$\mathcal{P}_{\mathtt{X}} = {\mathcal{C}_{\mathtt{X}}}^{9,995,987} \pmod{15,002,557}.$$

Наприклад, для першого слова `5330549` необхідно виконати операцію

$$\mathcal{P}_{\mathtt{X}} = 5,330,549^{9,995,987} \pmod{15,002,557}.$$

Це означає, що число, яке перевищує 5 мільйонів, треба піднести до степеня, який майже дорівнює 10 мільйонам, а потім знайти остачу від ділення на число, яке перевищує 15 мільйонів. Сучасні алгоритми та комп'ютери дозволяють це зробити майже миттєво. Ситуація змінюється докорінно, якщо k є невідомим: цю операцію треба виконати для кожної групи в шифрованому тексті й повторити це для всіх k. Як довго треба чекати результату дешифрування, якщо невідомими є показник k та модуль n?

3. Надійність експоненціальних шифрів

Уявімо, наприклад, що модулем експоненційного шифру $E_{k,n}$ є $n = 944,871,836,856,449,473$. Для дешифрування необхідно обчислити $\phi(944,871,836,856,449,473)$. Як ми знаємо, значення функції Ойлера для аргументу n легко обчислити, якщо знати його канонічне представлення у вигляді добутку простих дільників. ⑳ Ми обмежуємось модулями одного з двох видів: $n = p$ або $n = pq$. Навіть при цьому обмеженні факторизацію

$$944,871,836,856,449,473 = 961,748,941 \times 982,451,653$$

знайти нелегко, оскільки кожен з цих двох простих дільників ㉑ майже дорівнює мільярду. Варто все ж таки відзначити, що знаходження зазначеної факторизації зараз не є проблемою для комп'ютера. З іншого боку, існують настільки великі числа, факторизувати які не під силу навіть найпотужнішим сучасним комп'ютерам, об'єднаним у мережу для здійснення параллельних обчислень.

Приклад 6. Число

310 7418240490 0437213507 5003588856 7930037346 0228427275
4572016194 8823206440 5180815045 5634682967 1723286782
4379162728 3803341547 1073108501 9195485290 0733772482
2783525742 3864540146 9173660247 7652346609

складається з 193 десяткових цифр. Оскільки його двійковий розклад містить 640 двійкових цифр, то воно називається RSA-640 (скорочення RSA стане зрозумілим у лекції 10).

8 листопада 2005 року спеціалісти німецького федерального агенства з питань інформаційних технологій змогли

факторизувати RSA-640. Виявилось, що воно розкладається у добуток двох простих (дуже великих) множників

1634733 6458092538 4844313388 3865090859 8417836700 3309231218
1110852389 3331001045 0815121211 8167511579

×

1900871 2816648221 1312685157 3935413975 4718967899 6851549366
6638539088 0271038021 0449895719 1261465571

Факторизація числа RSA-640 відбулася через 2 роки з початку досліджень, причому задача була всісвітньо відомою й багато колективів намагались її розв'язати. Це означає, що задача факторизації числа RSA-640 є дуже складною з точку зору часу комп'ютерних обчислень, які необхідні для її розв'язання.

Для криптології це означає, що до 8 листопада 2005 року будь-яке повідомлення, зашифроване експененціальним шифром з модулем RSA-640, було неможливо прочитати непосвяченій стороні, навіть якщо їй було відомо, що шифрування здійснювалось саме для модуля RSA-640! ㉒

Такою ж відомою зараз є задача про факторизацію чисел RSA-704, RSA-768, RSA-896, RSA-1024, RSA-1536 та RSA-2048. За факторизацію кожного з них пропонується грошова премія: вона становить $200,000 у випадку RSA-2048.

Зауваження 3. Варто також додати, що після успішної факторизації числа n (після знаходження двох його дільників p та q) задача не закінчується, оскільки необхідно перевірити, що кожен з дільників є простим числом. Для великих чисел і ця задача є складною з точки зору обчислень Більш детально ми розглянемо її у лекції 12. Зараз лише зауважимо, що задача перевірки чисел на простоту в сучасних умовах розв'язується у нетрадиційний спосіб: відповідь

на питання про простоту великих чисел отримується лише з певною ймовірністю.

У лекції 10 ми розглянемо один з класичних методів факторизації чисел вигляду $n = pq$, який називається алгоритмом Ферма. Метод Ферма є ефективним, якщо дільники числа n є достатньо близькими до $\sqrt{n}$.

3.1. Метод факторизації Крайчика. Узагальнення методу Ферма було знайдено М. Крайчиком у 1926 році. Замість пар (x, y), які мають властивість $x^2 - y^2 = n$ і на якій базується метод Ферма, він запропонував шукати пари, які задовольняють більш загальне співвідношення $x^2 \equiv y^2 \pmod{n}$. В 1981 з'явився алгоритм наступного покоління, який розробив Д. Диксон з використанням ідей Крайчика.

Спочатку ми познайомимось з методом Крайчика на конкретному прикладі, а потім розглянемо загальний випадок.

Приклад 7. Покажемо як факторизувати число $n = 18601$ методом Крайчика. Будемо використовувати поліном другого степеня $Q(x) = x^2 - n$. Покладемо $x_0 = [\sqrt{n}]$ ($x_0 = 136$ у випадку $n = 18601$). ㉓ Позначимо $x_k = x_0 + k$ для $k \geq 1$ й обчислимо числа $Q_k = Q(x_k)$ для перших п'яти k:

k	1	2	3	4	5
x_k	137	138	139	140	141
Q_k	$168 = 2^3 \cdot 3 \cdot 7$	443	$720 = 2^4 \cdot 3^2 \cdot 5$	$999 = 3^3 \cdot 37$	$1280 = 2^8 \cdot 5$

㉔ Зауважимо, що $Q_3 Q_5 = 2^{12} \cdot 3^2 \cdot 5^2 = 960^2$, тобто $Q_3 Q_5$ є повним квадратом. За означенням чисел Q_k цю властивість

можна записати таким чином:

$$\begin{gathered}(139^2 - n)(141^2 - n) = 960^2, \quad \text{або} \\ (139^2 - n)(141^2 - n) \equiv 960^2 \pmod{n}, \quad \text{або} \\ 139^2 \cdot 141^2 \equiv 960^2 \pmod{n},\end{gathered}$$

тобто ми знайшли розв'язок конгруенції $x^2 \equiv y^2 \pmod{n}$ для $y = 960$. ㉕ Цим розв'язком є $x \equiv 139 \cdot 141 \pmod{n}$, тобто $x = 998$. ㉖ Тепер підрахуємо найбільші спільні дільники: ㉗

$$\begin{aligned}(n, x + y) &= (18601, 960 + 998) = 979, \\ (n, y - x) &= (18601, 998 - 960) = 19.\end{aligned}$$

Нескладно перевірити, що $18601 = 979 \cdot 19$.

Зауваження 4. Числа $Q_k = Q(x_k)$ є достатньо малими у порівнянні з n, якщо k є відносно малим. ㉘ Саме ця властивість пояснює наш вибір $x_k = x_0 + k$, хоча в алгоритмі Крайчика можна використати будь-яку іншу послідовність натуральних чисел $\{x_k\}$.

Найбільшим недоліком алгоритму Крайчика є те, що він використовує метод спроб та помилок. Для реалізації на комп'ютері такий метод зазвичай не є ефективним, тому у сучасних комп'ютерних програмах метод Крайчика не є популярним.

У загальному випадку алгоритм Крайчика знаходження дільників натурального числа можна описати наступним чином.

Алгоритм 1. Алгоритм факторизації Крайчика

Вхідні дані: складене натуральне число n;

Вихідні дані: дільники $n_1 \mid n$ та $n_2 \mid n$;

обчислити $x_0 = \left[\sqrt{n}\right]$; покласти $m = 1$;

`Вибір нового` m:

збільшити m на одиницю;

для $x_k = x_0 + k$, $k = 1, 2, \ldots, m$, обчислити $Q_k = x_k^2 - n$;

`Вибір підмножини індексів`:

обрати новий набір індексів $i_1, \ldots, i_s \subseteq \{1, \ldots, m\}$;

якщо добуток $Q_{i_1} \ldots Q_{i_s} \stackrel{\text{def}}{=} y^2$ є повним квадратом та

$(x \pm y, n) \neq 1$, де $x \stackrel{\text{def}}{=} x_{i_1} \ldots x_{i_s}$, то

$n_1 \stackrel{\text{def}}{=} (x - y, n)$ та $n_2 \stackrel{\text{def}}{=} (x + y, n)$ є дільниками n; `STOP`.

інакше повернутись до `Вибору підмножини індексів`;

Зауваження: якщо на кроці `Вибір підмножини індексів`

всі підмножини індексів $i_1, \ldots, i_s \subseteq \{1, \ldots, m\}$

вже перевірено, але повний квадрат не знайдено,

то перейти до кроку `Вибір нового` m.

Доведення алгоритму Крайчика. Якщо для певного набору індексів $i_1, \ldots, i_s$ число $Q_{i_1} \ldots Q_{i_s} \stackrel{\text{def}}{=} y^2$ є повним квадратом, то знайдено розв'язок $x = x_{i_1} \ldots x_{i_s}$ конгруенції

$$x^2 \equiv y^2 \pmod{n}, \tag{3}$$

оскільки $(x_{i_1}^2 - n) \ldots (x_{i_s}^2 - n) \equiv y^2 \pmod{n}$ за означенням послідовності $\{Q_i\}$. ㉙ Тому з (3) випливає, що $n \mid (x^2 - y^2)$. Якщо $(n, x \pm y) = 1$, то $n = n_1 n_2$. Інакше знайдеться натуральне число n_3, для якого $n = n_1 n_2 n_3$. ㉚ $\square$

Зауваження 5. Якщо $n = pq$, а p та q є простими числами, то алгоритм Крайчика знаходить саме p та q (в цьому випадку $n_3 = 1$). Якщо в результаті виконання алгоритму Крайчика виявиться, що $n_1 n_2 < n$, тобто $n = n_1 n_2 n_3$ й $n_3 > 1$, то алгоритм можна повторити, щоб знайти факторизацію числа n_3.

4. Односторонні функції

Перевірка правильності факторизації RSA-640 є рутинною задачею. Навіть без комп'ютера це можна зробити методом множення у стовпчик. ㉛ З іншого боку, обернена операція — факторизація числа — є складною.

Означення 1. Функція, значення якої обчислити доволі легко для будь-яких аргументів, називається *односторонньою*, якщо відновити аргументи за значенням функції дуже складно.

Як ми бачили вище, прикладом односторонньої функції є множення двох простих чисел.

4.1. Односторонні функції з секретом. Це такі односторонні функції, які мають додаткову властивість: якщо відома певна додаткова інформація, то обчислення аргументу за значенням функції стає простою задачею.

Однією з таких функцій є

$$f(x) = x^2 \pmod{n}, \quad \text{якщо} \quad n = pq,$$

де p та q є простими числами. Вона називається *функцією Рабіна*. Додатковою інформацією, яка робить обчислення x за значенням $f(x)$ простими, є знання p та q. Справедливим

є також і обернене твердження: задача факторизації числа n стає простою, якщо вміти обчислювати x за $f(x)$.

Іншу односторонню функцію з секретом ми будемо детально розглядати в лекції 10.

4.2. Дискретний логарифм. Ще однією односторонньою функцією є *дискретний логарифм* за модулем n та базою a, який позначається $\mathrm{dlog}_{a,n}(h)$ для аргументу h. Дискретний логарифм є розв'язком задачі

$$a^{\mathrm{dlog}_{a,n}(h)} \equiv h \pmod{n}, \qquad h \in \{0,1,2,\ldots,n-1\}. \tag{4}$$

Означення 2. Нехай a та n натуральні числа. Дискретним логарифмом цілого числа $x \in \{0,1,2,\ldots,n-1\}$ за модулем n та базою a називається таке ціле число $\mathrm{dlog}_{a,n}(h) \in \{0,1,2,\ldots,n-1\}$, для якого виконано рівність (4).

Назва пояснюється аналогією зі звичайним логарифмом за базою a, який позначається $\log_a(h)$ і є розв'язком задачі:

$$a^{\log_a(h)} = h, \qquad h > 0.$$

Ми фактично вже зустрічались з дискретними логарифмами, а саме ми назвали число j показником кореня k-ого степеня за модулем n, якщо

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

(див. формулу (8.5)). З використанням позначення для дискретного логарифма, попередню рівність можна записати наступним чином ㉜

$$1 + \mathrm{dlog}_{a,n}(1) = k \cdot j \pmod{n}.$$

Зауваження 6. Дискретний логарифм існує не при всіх комбінаціях a та n. Наприклад, якщо a та n є взаємно простими, то $\mathrm{dlog}_{a,n}(0)$ не існує. ㉝ Більше того, $\mathrm{dlog}_{a,n}(0)$ існує тільки тоді, коли одне з чисел a або n ділиться на інше. ㉞

Приклад 8. Обчислимо дискретний логарифм 6 за основою 31 та з базою 3, тобто обчислимо $\mathrm{dlog}_{3,31}(6)$.

Оскільки $3^0 \not\equiv 6 \pmod{31}$, то $\mathrm{dlog}_{3,31}(6) \neq 0$. ㉟ Аналогічно, $\mathrm{dlog}_{3,31}(6) \neq 1$. Продовжуючи ці обчислення для $x = 2, 3, \ldots$, тільки при $x = 25$ отримаємо $3^x \equiv 6 \pmod{31}$, тобто $\mathrm{dlog}_{3,31}(6) = 25$.

4.3. Алгоритм Шенкса. Більш ефективним для знаходження дискретного логарифма, ніж простий перебір, є алгоритм Шенкса. Нижче ми наводимо спрощений алгоритм Шенкса, який напевно дає результат, якщо n є простим числом, а a є примітивним коренем за модулем n. Існує модифікація цього алгоритму для загального випадку, але ми її не розглядаємо.

Означення 3. Нехай n є натуральним числом. Натуральне число a називається *примітивним* або *первісним коренем* за модулем n, якщо

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

та

$$a^l \not\equiv 1 \pmod{n} \quad \text{для будь-якого} \quad 1 \leq l < \phi(n).$$

Зауважимо, що примітивні корені існують не для всіх n, а тільки для $n = 2, 4, p^\alpha, 2p^\alpha$. Існування примітивного кореня для простих n довів К. Гаусс, але він сам писав, що цим поняттям користувався ще Л. Ойлер. Оскільки n є простим числом в алгоритмі, наведеному нижче, то примітивний корень за модулем n існує.

Через $\lceil x \rceil$ ми позначаємо найменше натуральне число, яке не є меншим за x.

Алгоритм 2. Алгоритм Шенкса

Вхідні дані: цілі числа a, n, h;
Вихідні дані: $\mathrm{dlog}_{a,n}(h)$;
обчислити $m = \lceil \sqrt{n} \rceil$ й $c \equiv a^{-m} \pmod{n}$;
обчислити $a^r \pmod{n}$, $r = 0, 1, \ldots, m-1$;
почати цикл з $q = 0$;
`Спроба знайти дискретний логарифм`:
якщо $hc^q \pmod{n} = a^r \pmod{n}$ для якогось r,
то $\mathrm{dlog}_{a,n}(h) = mq + r$ `STOP`.
Якщо ж $hc^q \pmod{n} \neq a^r \pmod{n}$ для будь-якого r,
то збільшити q на одиницю
та повторити `Спробу знайти дискретний логарифм`.

Доведення алгоритму Шенкса. Позначимо $m = \lceil x \rceil$, $x = \mathrm{dlog}_{a,n}(h)$. Поділимо x на m з остачею: $x = mq + r$ для деяких $q \geq 0$ та $0 \leq r < m$. Тому

$$h \equiv a^x = (a^m)^q \cdot a^r \pmod{n},$$

звідки $h\,(a^{-m})^q \equiv a^r \pmod{n}$. ㊱ Саме ці числа q та r знаходить алгоритм Шенкса, а за ними обчислює $\mathrm{dlog}_{a,n}(h)$. ㊲ □

Приклад 9. Обчислимо $\mathrm{dlog}_{3,31}(6)$ за алгоритмом Шенкса. Перш за все впевнімось, що $a = 3$ є примітивним коренем за модулем $n = 31$. Оскільки $\phi(31) = 30$, то для цього

необхідно здійснити наступні обчислення:

l	1	2	3	4	5	6	7	8	9	10
$3^l \pmod{31}$	3	9	27	19	26	16	17	20	29	25
l	11	12	13	14	15	16	17	18	19	20
$3^l \pmod{31}$	13	8	24	10	30	28	22	4	12	5
l	21	22	23	24	25	26	27	28	29	30
$3^l \pmod{31}$	15	14	11	2	6	18	23	7	21	1

㊳ Оскільки $3^l \equiv 1 \pmod{31}$ в множині $\{1, 2, \ldots, \phi(31)\}$ тільки для $l = 30$, то $a = 3$ дійсно є примітивним коренем за модулем $n = 31$. Тепер $m = \lceil \sqrt{n} \rceil = 6$ й $2 \equiv 3^{-6} \pmod{31}$, оскільки $2 \cdot 3^6 = 1458 = 47 \cdot 31 + 1$. ㊴ Далі обчислюємо $a^r \pmod{n}$, $r = 0, 1, \ldots, m-1$:

(5)

r	0	1	2	3	4	5
$3^r \pmod{31}$	1	3	9	27	19	26

㊵

Нарешті обчислюємо $6 \cdot 2^q \pmod{31}$:

q	0	1	2	3	4
$6 \cdot 2^q \pmod{31}$	6	12	24	17	3

㊶

Для кожного $q \geq 0$ шукаємо число $6 \cdot 2^q \pmod{31}$ в таблиці (5). Тільки для $q = 4$ ми отримали співпадіння числа $6 \cdot 2^q \pmod{31}$ з одним з елементів попередньої таблиці, а саме $6 \cdot 2^4 \pmod{31} = 3^1 \pmod{31}$. Таким чином, $\mathrm{dlog}_{3,31}(6) = mq + r$, тобто $\mathrm{dlog}_{3,31}(6) = 25$. ㊷

5. Контрольні питання

1. Перевірити, що $33^2 < k < 33^3$. (стор. 184).

2. Чому зроблено висновок про те, що групи складались з двох букв? (стор. 184).

3. Чому згадується саме група ЮБ? (стор. 185).

4. Чому ми вважаємо, що $n > 664$? (стор. 186).

5. Розкласти на множники числа 665 та 666. (стор. 186).

6. Перевірити, що $667 = 23 \cdot 29$. (стор. 186).

7. Пояснити чому ми вважаємо, що $n = pq$ для деяких простих чисел p та q? (стор. 186).

8. Чому для дешифрування необхідно перевірити всі степені $k \leq n$, які є взаємно простими з $\phi(n)$? (стор. 187).

9. Пояснити чому $\phi(616) = 240$? (стор. 187).

10. Для обчислення $3^{-1} \pmod{667} = 411$ використати розширений алгоритм Евкліда. (стор. 187).

11. Зробити необхідні обчислення для дешифрування. (стор. 187).

12. Чому потрібно перевіряти саме 240 варіантів для показника шифру? (стор. 187).

13. Чому наступним кандидатом для модуля шифру є саме число 669? (стор. 187).

14. Чому для експоненціального шифру $E_{k,8537}$ необхідно перевірити саме 8536 показників? (стор. 188).

15. Спробуйте застосувати частотний аналіз. (стор. 188).

16. Перевірити факторизацію $15,002,557 = 2447 \cdot 6131$. Чи є 2447 та 6131 простими числами? (стор. 189).

17. Чому $\phi(15,002,557) = 14,993,980$? (стор. 189).

18. Довести, що $3^{-1} \pmod{14993980} = 9,995,987$? (стор. 189).

19. Чому саме таку операцію? (стор. 189).

20. Пригадайте як обчислюється значення функції Ойлера, якщо відомим є канонічний розклад у добуток простих дільників аргументу функції. (стор. 189).

21. Чому 961,748,941 та 982,451,653 є простими числами? (стор. 190).

22. Пояснити це докладніше! (стор. 191).

23. Обчислити x_0 у прикладі 7. (стор. 192).

24. Перевірити обчислення та факторизацію Q_k. (стор. 192).

25. Пояснити конгруенцію $x^2 \equiv y^2 \pmod{n}$. (стор. 193).

26. Знайти розв'язок конгруенції $x \equiv 139 \cdot 141 \pmod{n}$. (стор. 193).
27. Підрахувати найбільші спільні дільники $(n, 998 + 960) = 979$ та $(n, 998 - 960) = 19$. (стор. 193).
28. Поясніть, що означає фраза "числа $Q_k = Q(x_k)$ є достатньо малими у порівнянні з n, якщо k є відносно малим"? (стор. 193).
29. Перевірити, що $x = x_{i_1} \dots x_{i_s}$ дійсно є розв'язком конгруенції (3). (стор. 194).
30. Чому знайдеться натуральне число n_3, для якого $n = n_1 n_2 n_3$, якщо $(n, x + y) \neq 1$ або $(n, x - y) \neq 1$? (стор. 194).
31. Напишіть програму для комп'ютера множення великих чисел та перевірте правильність факторизації числа RSA-640. (стор. 195).
32. Перевірити рівність $1 + \operatorname{dlog}_{a,n}(1) = k \cdot j \pmod{n}$. (стор. 196).
33. Чому $\operatorname{dlog}_{a,n}(0)$ не існує, якщо a та n є взаємно простими? (стор. 196).
34. Довести, що $\operatorname{dlog}_{a,n}(0)$ існує тільки тоді, коли одне з чисел a або n ділиться на інше. (стор. 196).
35. Чому $\operatorname{dlog}_{3,31}(6) \neq 0$? (стор. 197).
36. Чому $h\left(a^{-m}\right)^q \equiv a^r \pmod{n}$? (стор. 198).
37. Чому алгоритм Шенкса працює коректно у випадку простого n? (стор. 198).
38. Перевірити обчислення $3^l \pmod{31}$. (стор. 199).
39. Обчислити $2 \equiv 3^{-6} \pmod{31}$. (стор. 199).
40. Перевірити обчислення $3^r \pmod{31}$. (стор. 199).
41. Перевірити обчислення $6 \cdot 2^q \pmod{31}$, $1 \leq l \leq 30$. (стор. 199).
42. Перевірити безпосередньо, що $\operatorname{dlog}_{3,31}(6) = 25$. (стор. 199).

6. Задачі для самостійної роботи

Задача 1. *Дешифрувати текст*

```
27 23 31 8 1 6
```

зашифрований $E_{3,37}$ шифром.

Задача 2. *Дешифрувати текст*

```
23 7 31 15 10 31 1 23
```

зашифрований $E_{3,41}$ шифром.

Задача 3. *Доведіть, що шифрація та дешифрація згідно $E_{11,31}$ шифру здійснюються однаковим алгоритмом.*

Задача 4. *Нехай $n = pq$, де p та q є простими числами. Доведіть, що константу j для дешифрації $E_{k,n}$ шифру можно визначити за формулою*

$$kj \equiv 1 \pmod{m},$$

де $m = [p-1, q-1]$ — найменше спільне кратне чисел $p-1$ та $q-1$.

Задача 5. *Повідомлення зашифровано за допомогою експоненціального шифру з модулем $n = 491$. Скільки степенів k необхідно перевірити для дешифрації повідомлення, якщо використовується метод грубої сили?*

Задача 6. *Скільки чисел k можна використовувати для експоненціального шифру $E_{k,437}$? Напишіть формулу для кількості можливих чисел k, які можна використовувати для експоненціального шифру $E_{k,n}$.*

Задача 7. *Нехай $n = pq$. Припустимо, що $x > \sqrt{n}$ є таким натуральним числом, що $y^2 \stackrel{\text{def}}{=} x^2 - n$ є повним квадратом.*

a) *Доведіть, що $p = x + y$, $q = x - y$.*
b) *Чи варто користуватись експоненціальним шифром $E_{k,n}$ з $n = 97343$?*
c) *Яку рекомендацію необхідно надати розробнику експоненціального шифру?*

Задача 8. *При виборі модуля $n = pq$ для експоненціального шифра необхідно мати на увазі наступну обставину. Якщо $p-1$ та $q-1$ мають великий спільний дільник, то $(p-1, q-1)$ є достатньо малим числом.*

a) *Пояснити, чому в цьому випадку найменше спільне кратне $u \stackrel{\text{def}}{=} [p-1, q-1]$ є малим числом у порівнянні з $\phi(n)$?*
b) *Довести, що для дешифрації можна обрати $j \equiv k \pmod{n}$.*
c) *Пояснити, чому задача обчислення j спрощується, якщо є малим числом у порівнянні з $\phi(n)$?*
d) *Яку рекомендацію необхідно надати розробнику експоненціального шифру?*

Задача 9. *Розглянемо критичний випадок задачі* 8, *коли* $(q-1) \mid (p-1)$.

a) *Довести, що в цьому випадку* $j \equiv k^{-1} \pmod{p-1}$.
b) *Обчислити* j, *якщо* $n = 11041$.

Задача 10. *Припустимо, що* $n \geq 2$, *а канонічний розклад* $\phi(n)$ *містить тільки малі прості числа. Тоді число* j *можна знайти методом грубої сили.*

a) *Нехай, наприклад,* $\phi(n) = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot 5^{\alpha_5}$. *Оцінити зверху кількість спроб для знаходження* j *методом грубої сили.*
b) *Яку рекомендацію необхідно надати розробнику експоненціального шифру?*

Задача 11. *Якщо обидва числа* q *та* $2q+1$ *є простими, то* q *називається числом Софі Жермейн. Досі невідомо чи є послідовність чисел Софі Жермейн скінченою, але використання таких чисел у криптографії дозволяє уникнути багатьох проблем.*

a) *Показати, що проблем, згаданих у задачах* 9 *та* 10, *можна позбутись, якщо* $p = 2q+1$.
b) *Довести, що* 2, 3, 5, 11, 23, 29, 41, 53, 83, 89 *є числами Софі Жермейн.*

Задача 12. *Нехай* n_1, n_2, n_3 *є попарно простими числами, а* m *є натуральним числом. Позначимо* $m_i \equiv m^3 \pmod{n_i}$, $i = 1, 2, 3$.

a) *Пояснити як китайська теорема про остачі допомагає обчислити* $M \equiv m^3 \pmod{n_1 n_2 n_3}$.
b) *Як дешифрувати повідомлення* m, *якщо знати* M?
c) *Яку рекомендацію необхідно надати розробнику експоненціального шифру?*

Задача 13. *Припустимо, що один і той же текст надіслано трьом різним особам, які отримали повідомлення* m_1, m_2 *та* m_3. *Припустимо, що текст було зашифровано за допомогою експоненціальних шифрів* E_{3,n_1}, E_{3,n_2} *та* E_{3,n_3}.

a) *Уважно прочитайте умови задачі* 12.
b) *Нехай* $n_1 = 517$, $n_2 = 697$, $n_1 = 667$, $m_1 = 131$, $m_2 = 614$, $m_3 = 127$. *Відновити повідомлення.*

Задача 14. *Повідомлення m зашифровано експоненціальними шифрами $E_{3,493}$ та $E_{5,493}$. Зашифрованими повідомленнями є 293 та 421 відповідно. Знайти m.*

Задача 15. *Одне і те ж повідомлення m зашифровано шифрами $E_{k_1,n}$ та $E_{k_2,n}$, причому $(k_1, k_2) = 1$. Тоді повідомлення m можна відновити з зашифрованого тексту $c_1 \equiv m^{k_1} \pmod{n}$ або $c_2 \equiv m^{k_2} \pmod{n}$. Як?*

Задача 16. *Нехай $n = 1591$. `Аліса` використовує експоненціальний шифр $E_{k,n}$ з найменшим можливим k. Вона отримала повідомлення $c = 1292$. Як дешифрувати це повідомлення за допомогою китайської теореми про остачі (теорема 5.5)?*

Задача 17. *За допомогою експоненціального шифра $E_{k,n}$ шифрується повідомлення $m \in \{0, 1, \ldots, n-1\}$. Зашифрованим повідомленням є $c \equiv m^k \pmod{n}$. Доведіть, що існує i, для якого*

$$m^{k^i} \equiv m \pmod{n}.$$

Доведіть, що для такого i виконується

$$c^{k^{i-1}} \equiv m \pmod{n}.$$

Чи зменшує така властивість небезпечність експоненціального шифра $E_{k,n}$?

Задача 18. *Припустимо, що $(p-1) \mid (k-1)$ та $(q-1) \mid (k-1)$. Довести, що*

a) *будь-яке повідомлення m шифрується в m за допомогою експоненціального шифру $E_{k,n}$;*
b) *пояснити, чому вибір $k = \phi(n)/2 + 1$ є особливо поганим для експоненціального шифру, хоча він задовольняє вимогам стосовно величини параметра k?*

Задача 19. *Для кожного експоненціального шифру існують тексти, які не змінюються при шифруванні. Таких текстів є принаймні чотири.*

Нехай m — це розв'язок системи лінійних конгруенцій:

$$m \equiv a \pmod{p}, \qquad m \equiv b \pmod{q}, \tag{6}$$

де $a, b \in \{+1, -1\}$.

a) *Чому система* (6) *має розв'язок?*
b) *Пригадати, чому параметр k експоненціального шифру $E_{k,n}$ є непарним числом?*
c) *Довести, що* $m \equiv m^k \pmod{pq}$, *де m — це розв'язок системи* (6).
d) *знайти чотири тексти, які не змінюються при шифруванні $E_{7,55}$ шифром.*

Задача 20. *Нехай c — це повідомлення m, яке було зашифровано за допомогою $E_{k,n}$ шифру. Припустимо, що r — це випадкове число. Нарешті, припустимо, що повідомлення $cr^k \pmod{n}$ вдається дешифрувати. Як відновити m?*

Задача 21. *За допомогою метода Крайчика факторизувати число* 12499.

Задача 22. *За допомогою метода Крайчика факторизувати число* 20437.

Задача 23. *За допомогою метода Шенкса знайти дискретний логарифм числа $h = 15$ за модулем $p = 29$ та базою $a = 2$.*

Задача 24. *За допомогою метода Шенкса знайти дискретний логарифм числа $h = 20$ за модулем $p = 47$ та базою $a = 5$.*

Задача 25. *Дешифрацію повідомлень в рамках мультиплікативних шифрів можна прискорити майже вдвічи, якщо використати китайську теорему про остачі.*

Нехай $n = pq$, де p та q є простими числами. Нехай k — це показник для шифрації, а j — показник для дешифрації у випадку експоненціального шифру $E_{k,n}$. Нехай $c \equiv m^k \pmod{n}$. Для дешифрації цього повідомлення обчислимо

$$c_p \equiv c^{j \pmod{p-1}} \pmod{p}, \qquad c_q \equiv c^{j \pmod{q-1}} \pmod{q}.$$

Після цього знаходимо $\lambda \in \{0, 1, \ldots, n-1\}$, *яке задовольняє наступну систему конгруенцій*

$$\lambda \equiv c_p \pmod{p}, \qquad \lambda \equiv c_q \pmod{q}.$$

a) *Чому існує розв'язок цієї конгруенції?*
b) *Довести, що* $\lambda = m$. *Як обчислити* λ?
c) *Припустимо, що відомі числа* x *та* y, *для яких* $xp + yq = 1$. *Як у цьому випадку знайти* λ?
d) *Як знайти* x *та* y?

Задача 26. *Повідомлення* m *зашифровано експоненціальним шифром* $E_{3,253}$, *результатом є* $c = 119$.

a) *Факторизувати* n.
b) *Знайти показник дешифрації* j.
c) *Обчислити* m *за допомогою* j.
d) *Обчислити* m *методом, описаним у задачі* 25.

Задача 27. *Ще одним надійним криптометодом є метод Рабіна. Щоб ним користуватись, необхідно обрати такі два великих простих числа* p *та* q, *що* $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$. *Тоді повідомлення* m *шифрується за правилом*

$$c \equiv m^2 \pmod{n},$$

де $n = pq$.

Для дешифрації повідомлення обчислюються числа

$$m_p \equiv c^{(p+1)/4} \pmod{p}, \qquad m_q \equiv c^{(q+1)/4} \pmod{q}.$$

Закінчення процедури дешифрації основано на китайській теоремі про остачі й нагадує метод, описаний в задачі 25: спочатку знаходимо x *та* y, *для яких* $xp + yq = 1$; *потім обчислюємо*

$$r \equiv (xpm_q + yqm_p) \pmod{n}, \qquad r \equiv (xpm_q - yqm_p) \pmod{n}.$$

Тоді одне з чисел $\pm r$, $\pm s$ *дорівнює* m.

a) *Чому такі прості числа* p *та* q *можна знайти?*

b) *Чому* $\pm m_p$ *є квадратним коренем з* c *за модулем* p, *а* $\pm m_q$ *є квадратним коренем з* c *за модулем* q?
c) *Чому розв'язок рівняння* $xp + yq = 1$ *існує? Як його знайти?*
d) *Чому кожне з чотирьох чисел* $\pm r$, $\pm s$ *є квадратним коренем з* c *за модулем* m?

Задача 28. *Криптосистема Рабіна (див. задачу* 27*) використовується з* $p = 11$ *та* $q = 23$, *тобто з* $n = 253$. *Повідомлення* m *шифрується в* $c \equiv m^2 \pmod{n}$, *тобто* $c = 170$. *Обчислити* m.

Задача 29. `Аліса` *грає з* `Бобом` *в "очко"* через Інтернет. Для цього вони спільно обрали дуже велике просте число* p *й різні (секретні) показники* k_A *та* k_B, *щоб використовувати приватні експоненціальні шифри* $E_{k_A,p}$ *та* $E_{k_B,p}$. *Крім того, вони узгодили нумерацію карт в колоді.*

Кожен раунд починається з того, що `Аліса` *перетасовує колоду карт (переставляє карти у випадкову порядку) й шифрує їх своїм шифром. Раунд продовжується наступним чином*:

i) `Аліса` *надсилає* `Бобу` *послідовність зашифрованих номерів*;
ii) `Боб` *обирає одне з чисел і повідомляє його* `Алісі`; *вона дешифрує це число і знає свою карту у цьому раунді*;
iii) `Боб` *обирає інше число з послідовності, шифрує його своїм шифром, результат надсилає* `Алісі`; *вона застосовує до отриманого числа свою операцію дешифрації і цей результат повертає* `Бобу`;
iv) `Боб` *застосовує до отриманого числа свою операцію дешифрації і дізнається, якою є його карта у цьому раунді.*

Дві карти, обрані у цьому раунді, вилучаються з колоди і у наступних не використовуються. Ця процедура продовжується допоки `Боб` *не зупиняє гру.*

a) *Чи не дізнається* `Боб` *про карту* `Алісн` *на кроці* ii)?
b) *Чи не дізнається* `Аліса` *про карту* `Боба` *на кроці* iii)?
c) *Чи правильно* `Боб` *визначає свою карту на кроці* iv)?
d) *Як після гри впевнитись, що гравці не мухлювали*?

---

*Англійською мовою "*blackjack*"

Задача 30. Аліса *надіслала* Бобу *повідомлення*:

21 27 49 19 45 42 27 49 25 19 29 21 27 7 27
43 25 30 33 20 32 21 45 30 25 14 42 45 19 27

зашифроване експоненціальним шифром $E_{7,53}$. Ева *не знає яким чином параметри шифру можна використати для дешифрації. Їй здається, що повідомлення містить текст* НІКОЛИ НЕ ПОГОДИТЬСЯ.

a) *Як їй впевнитись у своїй гіпотезі*?
b) *Чи зможе вона дешифрувати повідомлення*?