Дискретна математика - 2

Змістовий модуль 7. Теорія чисел і криптографія

Тема 8. Класична криптографія. Криптосистеми з відкритим ключем

План лекції

- Класична криптографія
- Криптосистеми з відкритим ключем
- Криптографічні протоколи

Класична криптографія

Шифри зсуву і афінні шифри

Одним із найбільш ранніх відомих користувачів криптографії був давньоримський імператор Юлій Цезар. Він зашифровував свої повідомлення у спосіб, коли кожна буква заміщується деякою іншою, а саме тою, що знаходиться в алфавіті через три позиції. Стосовно української абетки це означає, що А міняється на Г, Б на Ґ, В на Д, Г на Е і т.д. Останні ж три букви абетки Ь, Ю та Я заміщуються буквами, що знаходяться через три позиції *циклічно*, тобто переходять у А, Б та В, відповідно. Щоб описати цей *шифр Цезаря* математично, спочатку замінимо кожну букву українського алфавіту елементом множини $\mathbf{Z}_{33}$, тобто цілим числом від 0 до 32: кожна буква замінюється своїм порядковим номером,

причому нумерація починається з 0. Наприклад, А міняється на 0, Ї – на 12, Я – на 32. Метод шифрування Цезаря можна подати функцією f, яка визначена на множині $\mathbf{Z}_{33}$ і набуває значення із цієї ж множини:

$$f(p)=(p+3)\ \mathbf{mod}\ 33.$$

Під час шифрування повідомлення буква, яка представлена p міняється на букву, представлену $(p+3)\ \mathbf{mod}\ 33$.

Приклад. Зашифруємо шифром Цезаря повідомлення «Я ПРИЇДУ ЗАВТРА». Спочатку замінимо кожну букву її номером, тоді одержимо:

32 19 20 10 12 5 23 9 0 2 22 20 0.

Тепер замінимо кожний із цих номерів p на $(p+3)\ \mathbf{mod}\ 33$, це дасть:

2 22 23 13 15 8 26 12 3 5 25 23 3.

Повертаючись тепер від цифр назад до букв, одержимо зашифроване повідомлення:

«В ТУЙЛЖЦ ЇГДХУГ».

Для одержання оригінального повідомлення із секретного, зашифрованого шифром Цезаря, використовують функцію f^{-1}, обернену до f. Ця функція відображає ціле число p із множини Z_{33} у $f^{-1}(p)=(p-3)\ \mathbf{mod}\ 33$. Процес знаходження оригінального повідомлення із зашифрованого називають *дешифруванням*.

Зауваження. У разі шифрування повідомлень, написаних англійською мовою, очевидно використовують функцію $f(p)=(p+3)\ \mathbf{mod}\ 26$, а для розшифрування – функцію $f^{-1}(p)=(p-3)\ \mathbf{mod}\ 26$. Область визначення та область значень обох функцій – множина $\mathbf{Z}_{26}$.

Шифр Цезаря можна узагальнити в різний спосіб. Наприклад, замість зсуву числового еквівалента кожної букви на 3, можна зсувати числовий еквівалент кожної букви на k, отже

$$f(p)=(p+k)\ \mathbf{mod}\ 33.$$

Такий шифр називають *шифром зсуву*. Зазначимо, що для розшифрування тут має бути використана функція $f^{-1}(p)=(p-k)\ \mathbf{mod}\ 33$. Тут ціле число k називають *ключем*.

Подальше узагальнення шифру зсуву, яке трохи посилює його стійкість до розкриття, є використання функції $f(p)=(ap+b)\ \mathbf{mod}\ 33$, де a та b цілі, які вибирають так, щоб функція f була **бієкцією**. (Для того, щоб функція $f(p)=(ap+b)\ \mathbf{mod}\ 33$ була бієкцією, необхідно й достатньо, щоб $\gcd(a,33)=1$). Таке відображення називають *афінним перетворенням*, а відповідний шифр – *афінним шифром*.

Приклад. Якою буквою буде замінена буква Ю, якщо для шифрування використати функцію $f(p)=(7p+3)\ \mathbf{mod}\ 33$? Оскільки 31 репрезентує букву Ю, то використовуючи задану шифрувальну функцію, дістанемо $f(31)=(7\cdot 31+3)\ \mathbf{mod}\ 33=22$. Оскільки 22 репрезентує букву Т, то в зашифрованому повідомленні Ю заміниться на Т.

Тепер покажемо, як розшифрувати повідомлення, яке зашифроване афінним шифром. Припустімо, що $c=(ap+b)\ \mathbf{mod}\ 33$, причому $\gcd(a,33)=1$. Для дешифрування нам потрібно показати, як виразити p через c. Щоб це зробити, розглянемо шифрувальну конгруенцію

$c \equiv ap + b \pmod{33}$ і розв'яжемо її відносно p. Щоб це зробити, спочатку віднімемо b від обох частин конгруенції, тоді матимемо $c - b \equiv ap \pmod{33}$. Тому що $\gcd(a, 33) = 1$, існує обернене a^{-1} до a за модулем 33. Помножимо обидві частини останньої конгруенції на a^{-1}, тоді одержимо $a^{-1}(c-b) \equiv a^{-1}ap \pmod{33}$. Оскільки $a^{-1}a \equiv 1 \pmod{33}$, то $p \equiv a^{-1}(c-b) \bmod 33$. Це визначає p, бо p належить $\mathbf{Z}_{33}$.

Блокові шифри

Шифри зсуву та афінні шифри міняють кожну букву алфавіту на іншу букву того ж алфавіту. Тому їх називають *моноалфавітними* шифрами. Розкриття таких шифрів успішно здійснюється аналізом частот появи букв у зашифрованому тексті. Зашифрований текст можна зробити більш стійким до розкриття, якщо при шифруванні заміняти **блоки** букв на інші **блоки** букв. Такі шифри називають *блоковими шифрами*.

Розглянемо простий тип блокового шифру, який називають *шифром перестановки*. Як ключ використовуватимемо перестановку σ множини $\{1, 2, \ldots, m\}$ для деякого додатного цілого m – це **ін'єктивна** функція із $\{1, 2, \ldots, m\}$ у цю ж множину. Для шифрування повідомлення ми спочатку розбиваємо його на блоки, кожний з яких містить по m букв. (Пробіли між буквами та знаки пунктуації ігноруються. Якщо кількість букв у повідомленні не ділиться на m, то останній блок доповнюємо в кінці випадковими буквами.) Блок $p_1 p_2 \ldots p_m$ шифруємо як $c_1 c_2 \ldots c_m = p_{\sigma(1)} p_{\sigma(2)} \ldots p_{\sigma(m)}$. Для розшифрування блоку $c_1 c_2 \ldots c_m$ криптотексту ми переставляємо його букви використовуючи перестановку σ^{-1}, обернену до перестановки σ.

Приклад. Застосуємо шифр перестановки з такою перестановкою σ множини $\{1, 2, 3, 4\}$: $\sigma(1)=3$, $\sigma(2)=1$, $\sigma(3)=4$, $\sigma(4)=2$. Зашифруємо повідомлення «Я ПРИЇДУ ЗАВТРА». Розбиваємо на блоки по чотири букви, останній блок доповнюємо випадковими буквами:

ЯПРИ ЇДУЗ АВТР АДЛГ.

Застосуємо для кожного блоку перестановку σ й отримаємо:

ПИЯР ДЗЇУ ВРАТ ДГАЛ.

Для дешифрування використаємо обернену перестановку: $\sigma^{-1}(1)=2$, $\sigma^{-1}(2)=4$, $\sigma^{-1}(3)=1$, $\sigma^{-1}(4)=3$.

Ще один тип блокового шифру – *шифр Віженера*. Відкритий текст і криптотекст записуються в одному й тому ж алфавіті. Для букв *x* та *y* цього алфавіту означимо їхню суму *x* + *y* як результат додавання номерів цих букв за модулем 26 для англомовного повідомлення і за модулем 33 – для україномовного. Нагадаємо що нумерація букв алфавіту починається з нуля.

Шифр Віженера застосовують до повідомлення, записаного в рядок без пропусків і розділових знаків. Ключем є слово в тому ж алфавіті. Якщо ключ коротший за повідомлення, то його записують багато разів поспіль, доки не вийде рядок такої ж довжини. Рядок із розмноженим ключем записують під рядком із повідомленням, і букви, що опинилися одна над одною, додають. Як результат отримують рядок тої ж довжини, який і є криптотекстом.

Для дешифрування потрібно від значень букв коду відняти значення букв ключа і результат щоразу редукувати за модулем 26 чи 33 залежно від алфавіту повідомлення.

Приклад. Шифрування наказу БОРОНІТЬ КОРОЛІВНУ ВІД ВОРОГІВ з ключем КЛЮЧ відбувається так

	Б	О	Р	О	Н	І	Т	Ь	К	О	Р	О	Л	І	В	Н	У	В	І	Д	В	О	Р	О	Г	І	В
+	К	Л	Ю	Ч	К	Л	Ю	Ч	К	Л	Ю	Ч	К	Л	Ю	Ч	К	Л	Ю	Ч	К	Л	Ю	Ч	К	Л	Ю
	Л	А	О	Ї	Ю	Ц	Р	Ф	Ш	А	О	Ї	Щ	Ц	А	І	Ґ	Н	З	Я	М	А	О	Ї	Н	Ц	А

Результатом шифрування є нижній рядок. Як можна побачити, при використанні шифру Віженера однаковим буквам у відкритому тексті можуть відповідати різні букви у криптотексті. Ця обставина, безперечно, ускладнює частотний криптоаналіз.

Історична довідка. У 20-х роках минулого століття були винайдені роторні шифрувальні пристрої, які вдосконалювались упродовж наступних десятиліть та інтенсивно використовувались під час ІІ світової війни. Прикладом може служити відомий німецький шифр *Enigma*. Роторні системи реалізовували багаторівневу композицію шрифтів Віженера, що давало шифр з дуже великим періодом.

Криптосистеми з відкритим ключем.

Усі класичні шифри, зокрема зсуву, афінні – це криптосистеми з секретним ключем. Відмінна особливість таких криптосистем полягає в тому, що кожний, кому відомий шифрувальний ключ, швидко може знайти ключ дешифрувальний. Отже, знання як зашифровано повідомлення з використанням секретного ключа дає змогу розшифрувати повідомлення, яке було зашифроване за допомогою цього ключа. Тому класичні криптосистеми називають *симетричними*.

Нині широко застосовують криптосистеми з відкритим ключем. Такі системи називають *асиметричними* – для шифрування й розшифрування вони використовують різні ключі. Ключ, що його використовують для шифрування, є відкритим (публічним) і може бути повідомлений усім бажаючим надіслати секретне повідомлення. Ключ для розшифрування – закритий (приватний) і зберігається таємно одержувачем шифрованих повідомлень. Навіть знання всього зашифрованого повідомлення й відкритого ключа не дає змоги дешифрувати повідомлення (без знання закритого ключа).

Система шифрування RSA

У 1976 р. дослідники з Массачусетського технологічного інституту Рональд Райвест (Ronald Rivest), Аді Шамір (Adi Shamir) та Леонард Адлеман (Leonard Adleman) запропонували систему шифрування з відкритим ключем, нині відому як **система RSA**, за першими буквами прізвищ її винахідників.

Коротко опишемо цю систему шифрування.

•**1.** Одержувач повідомлень здійснює генерування відкритого ключа (пара чисел n та e) і секретного ключа (число d). Для цього:

- вибирають два простих числа p і q;
- обчислюють першу частину відкритого ключа $n = pq$;
- визначають другу частину відкритого ключа – вибирають невелике непарне число e, яке має бути взаємно простим з числом $(p-1)(q-1)$;
- обчислюють секретний ключ d, який є цілим числом, оберненим до e за модулем $(p-1)(q-1)$: $d = e^{-1}$ **mod**$((p–1)(q–1))$, тобто $de \equiv 1$ (mod$(p–1)(q–1)$); таке обернене існує, бо gcd $(e, (p – 1)(q – 1)) = 1$.

•**2.** Повідомлення перетворюють у цифрову форму, тобто записують у вигляді послідовності цілих чисел. Щоб це зробити, ми спочатку замінюємо кожну букву повідомлення на двоцифрове число, використовуючи ту саму заміну, що й для шифру зсуву, але з однією відмінністю. А саме, ми включимо початковий нуль для букв від А до З (в українській абетці), отже А заміниться на 00, Б – на 01, …, З – на 09. Після цього ми об’єднуємо ці двоцифрові числа в цифровий рядок. Нарешті, ми розбиваємо цей рядок на

рівного розміру **блоки** з $2N$ цифр, де $2N$ – найбільше додатне число таке, що 3232…32 (для українського алфавіту), чи 2525…25 (для англійського) із $2N$ цифр не перевищує n. У разі необхідності ми доповнюємо повідомлення фіктивним символом так, щоб останній блок мав такий самий розмір, що й інші. Отже, повідомлення подано як послідовність блоків M_1, M_2, …, M_k для якогось цілого k.

Шифрування полягає в трансформації кожного блоку M_i у зашифрований блок C_i. Це робиться з використанням функції

$$C = M^e \bmod n.$$

Для виконання шифрування ми використовуємо алгоритм швидкого піднесення до степеня в модулярній арифметиці (алгоритм 4.1).

Ми одержуємо зашифроване повідомлення як послідовність блоків цілих чисел і відправляємо її бажаному одержувачу. Тому що криптосистема RSA перетворює блоки букв у блоки букв, вона є **блоковим шифром**.

•3. Одержувач розшифровує повідомлення за допомогою секретного ключа d. Це здійснюють для кожного зашифрованого блоку C_i за допомогою функції

$$M = C^d \bmod n$$

Зазначимо, що для дешифрування використовують той самий алгоритм швидкого піднесення до степеня в модулярній арифметиці (алгоритм 4.1), що й для шифрування.

Перед тим, як обґрунтувати коректність розглянутої системи шифрування, наведемо елементарний приклад. Для обчислень у модулярній арифметиці можна скористаємося онлайн модулярним калькулятором.

Приклад.

Генерування ключів.

1.Вибираємо $p = 53$, $q = 67$.

2. $n = pq = 53 \cdot 67 = 3551$.

3. $(p - 1)(q - 1) = 52 \cdot 66 = 3432$, $e = 17$.

4. $d = e^{-1} \bmod (52 \cdot 66) = 17^{-1} \bmod 3432 = 1817$; для обчислення можна скористатись розширеним алгоритмом Евкліда та теоремою Безу або онлайн модулярним калькулятором.

Шифрування повідомлення. Нехай потрібно передати вказівку КУПИ. Спочатку перетворюємо повідомлення в цифрову форму, замінюючи кожну букву її двоцифровим номером в алфавіті (нагадаємо, що нумерація починається з 0: буква А заміниться на 00); отримаємо 14231910. З нашим модулем $n = 3551$ цифрове повідомлення розбивається на блоки по чотири цифри, бо $3232 < 3551 < 323232$:

1423 1910 (тобто $M_1 = 1423,\ M_2 = 1910,\ k = 2$).

Ми шифруємо кожен блок M_i, використовуючи функцію $C = M^e \bmod n$. Обчислення за допомогою алгоритму швидкого піднесення до степеня в модулярній арифметиці або за допомогою онлайн модулярного калькулятора дають $1423^{17} \bmod 3551 = 3153$, $1910^{17} \bmod 3551 = 2335$. Зашифроване повідомлення 3153 2335 (тобто $C_1 = 3153,\ C_2 = 2335$).

Розшифрування повідомлення. Кожний блок шифру C_i розшифровуємо, використовуючи функцію $M = C^d \bmod n$. Обчислення за допомогою алгоритму швидкого піднесення до степеня в модулярній арифметиці або за допомогою онлайн модулярного калькулятора дають $3153^{1817} \bmod 3551 = 1423,\ \ 2335^{1817} \bmod 3551 = 1910$. Ми одержали вихідне повідомлення у цифровій формі:1423 1910. Повертаючись до букв українського алфавіту, одержуємо вихідне повідомлення КУПИ.

Обґрунтування коректності системи RSA.

Нагадаємо, що $de \equiv 1 \pmod{(p-1)(q-1)}$, тому існує ціле j таке, що $de = 1 + j(p-1)(q-1)$. Звідси випливає, що

$$C^d \equiv \left(M^e\right)^d \equiv M^{de} \equiv M^{1+j(p-1)(q-1)} \pmod{n}.$$

Зазначимо, що $M^{1+j(p-1)(q-1)} = M \cdot \left(M^{p-1}\right)^{j(q-1)} = M \cdot \left(M^{q-1}\right)^{j(p-1)}$.

Подальше обґрунтування зробимо в додатковому припущенні, що

$$\gcd(M, p) = \gcd(M, q) = 1,$$

яке виконується за виключенням рідких випадків.

Тоді за малою теоремою Ферма можемо записати

$$C^d \equiv M \cdot \left(M^{p-1}\right)^{j(q-1)} \equiv M \cdot 1 = M \pmod{p},$$

$$C^d \equiv M \cdot \left(M^{q-1}\right)^{j(p-1)} \equiv M \cdot 1 = M \pmod{q}.$$

Оскільки $\gcd(p,q) = 1$, то з китайської теореми про остачі випливає, що $C^d \equiv M \pmod{pq}$.

Чому криптосистема RSA підходить для криптографії з відкритим ключем?

По-перше, можна швидко побудувати відкритий ключ, знайшовши два великих простих числа p і q, кожне з яких має більш ніж 200 цифр, і знайти ціле число e, взаємно просте з $(p-1)(q-1)$. Коли ми знаємо розклад n на множники, тобто, коли ми знаємо p і q, ми можемо швидко знайти d, яке є цілим, оберненим до e за модулем $(p-1)(q-1)$. [Це робиться за допомогою алгоритму Евкліда: знаходять коефіцієнти Безу s і t для e і $(p-1)(q-1)$, тоді s – обернене до e за модулем $(p-1)(q-1)$.]

Знання d дає змогу розшифрувати повідомлення, відправлені за допомогою нашого ключа. Однак, невідомий спосіб розшифрування повідомлень, який не заснований на пошуку факторизації n (тобто розкладу n на прості множники). Факторизація вважається важким завданням, на відміну від знаходження великих простих чисел p і q, **яке може бути зроблено швидко за допомогою імовірнісних методів**. Найбільш відомі (станом на 2018 р.) ефективні методи факторизації вимагають мільярди років для факторизації 400-значних чисел. Отже, якщо p і q 200-розрядний прості числа, то вважається, що повідомлення, зашифровані за допомогою $n = pq$, не можуть бути розшифровані в розумний період часу, за виключенням ситуації, коли прості числа p і q відомі.

Звичайно, коли числа p і q невеликі, як-от у нашому навчальному прикладі, задача факторизації n не є складною і такий шифр неважко розкрити.

Криптографічні протоколи

Досі ми вивчали, як криптографію можна використати, щоб засекретити повідомлення. Проте, є й інші важливі застосування криптографії. Одне з них – криптографічні протоколи, які дають змогу досягти певного рівня безпеки при обміні повідомленнями між сторонами або учасниками протоколу. Під протоколом ми будемо розуміти послідовність узгоджених приписів, згідно з якими відбувається обмін повідомленнями. Зокрема, ми покажемо, як можна використати криптографію, щоб дати змогу двом сторонам обмінюватись секретним

ключем через незахищений канал зв'язку. Ми покажемо також, як криптографію можна використати для відправлення підписаних секретних повідомлень таким чином, щоб одержувач міг бути впевненим, що повідомлення прийшло від передбачуваного відправника.

Обмін ключем

Класична симетрична система захисту конфіденційності листування ґрунтується на наявності надійного каналу для обміну секретним ключем. Канал цей може бути набагато повільнішим, ніж канал для обміну повідомленнями, але безумовно він має бути захищеним від посягань суперника. У класиці такий канал реалізовували за допомогою кур'єра.

В асиметричних криптосистемах проблеми пересилання ключа не існує, бо секретний ключ є особистою власністю кожної сторони, а відкритий ключ перебуває у відкритому доступі. Зазначимо однак, що з появою асиметричних криптосистем симетричні системи не вийшли зі вжитку, бо вони є набагато швидкішими. Фактор швидкості шифрування або дешифрування стає визначальним при пересиланні великих обсягів інформації. Проте асиметричні криптосистеми відкривають нові можливості для обміну ключами при використанні криптосистем симетричних. Наприклад, практичним є пересилання ключа тим же каналом зв'язку, що й звичайних повідомлень, але зашифрованого за допомогою асиметричної криптосистеми. І хоча швидкодія криптосистеми з відкритим ключем нижча, для цієї мети вона достатня, адже ключ буде посилатися значно рідше, ніж звичайні повідомлення.

Нижче наводиться **інше** елегантне розв'язання проблеми, а саме, *протокол експоненціального обміну ключем*. Двоє учасників протоколу – їх за усталеною традицією звуть Аліса і Боб – спілкуються через канал, що ймовірно прослуховується, і тому хочуть

домовитися про спільний секретний ключ. Протокол, за яким вони діятимуть, містить такі кроки, де обчислення виконуються в Z_p.

(1) Аліса вибирає велике просте число p і первісний корінь r за модулем p, і **відкрито**, не роблячи з цього жодної таємниці, посилає p і r Бобові.

(2) Аліса вибирає **секретне** число k_1 у межах від 1 до $p-1$ включно, а Боб – **секретне** число k_2 у тих же межах.

(3) Аліса обчислює r^{k_1} **mod** p і **відкрито** посилає це значення Бобові, а Боб обчислює r^{k_2} **mod** p і теж **відкрито** посилає Алісі.

(4) Аліса обчислює число $\left(r^{k_2}\right)^{k_1}$ **mod** p.

(5) Боб обчислює число $\left(r^{k_1}\right)^{k_2}$ **mod** p.

Як результат – Аліса і Боб обчислюють одне і теж число $\left(r^{k_2}\right)^{k_1}$ **mod** $p = \left(r^{k_1}\right)^{k_2}$ **mod** $p = r^{k_1 k_2}$ **mod** p, яке і приймають у якості **секретного** ключа.

Бачимо, що p, r, r^{k_1} **mod** p, r^{k_2} **mod** p – передбачається як відкрита інформація, а k_1, k_2 та спільний ключ $r^{k_1 k_2}$ **mod** p – як інформація секретна. Для видобування секретної інформації з відкритої суперникові потрібно розв'язати конкретну задачу обчислення дискретного логарифму. Справді, суперникові потрібно знайти k_1 і k_2 із r^{k_1} **mod** p і r^{k_2} **mod** p, відповідно. Жодний інший спосіб видобути цю секретну інформацію із відкритої невідомий. У свій час ми наголошували, що задача обчислення дискретного логарифму є практично нерозв'язною, коли числа p і r є достатньо великими. За досяжної нині потужності комп'ютерів ця система

вважається незламною, коли p має більше 300 десяткових цифр, а k_1 і k_2 – більше 100 десяткових цифр кожне.

Цифровий підпис

Нині певні фінансові операції мають здійснюватись за короткий період часу, що унеможливлює використання традиційних засобів засвідчення платіжних документів на зразок великої гербової печатки та підпису головного бухгалтера. Але як тоді банкові вберегтися від злодія-інтелектуала, який добре знається і на фінансах, і на електроніці, і може від імені співробітника банку надіслати вимогу перевести гроші на власний підставний рахунок? Тут ми покажемо, як криптографію можна використати для того, щоб особа, яка отримала інформацію, була впевненою, що ця інформація отримана саме від відомої їй людини. Це питання вирішується за допомогою *протоколу цифрового підпису*. Ми розглянемо конкретну реалізацію такого протоколу на базі системи RSA.

Нехай (n, e) – відкритий ключ Аліси, а d – секретний. Аліса може шифрувати повідомлення x, використовуючи *шифрувальну* функцію $E_{(n,e)}(x) = x^e \bmod n$ і може розшифровувати шифроване повідомлення y, використовуючи *дешифрувальну* функцію $D_{(n,e)}(y) = y^d \bmod n$.

Зазначимо, що Аліса бажає надіслати повідомлення так, щоб кожний, хто його отримає, був упевнений, що це повідомлення саме від неї. Так само, як і під час RSA-шифрування, вона переводить букви повідомлення (незашифрованого) у цифрові еквіваленти і розділяє отриманий цифровий рядок на блоки M_1, M_2, …, M_k рівного розміру (розмір блоків визначають точно так, як і при RSA-шифруванні). Після цього вона застосовує свою

дешифрувальну функцію $D_{(n,\,e)}$ до кожного блоку і дістає $D_{(n,\,e)}(m_i)$, де $i = 1, 2, \ldots, k$. Аліса посилає цей результат усім запланованим адресатам.

Коли будь-який адресат отримує її лист, він застосовує Алісину **шифрувальну** функцію $E_{(n,\,e)}$ до кожного отриманого блока цифр, – це доступно для будь-кого, бо Алісин відкритий ключ (n, e) – доступна інформація. Результат – блок повідомлення, яке пересилалось, бо $E_{(n,\,e)}\left(D_{(n,\,e)}(M_i)\right) = M_i$. Отже, Аліса має змогу надсилати свої листи багатьом адресатам, і, якщо вона діятиме за описаним протоколом, кожний адресат може бути впевненим, що лист прийшов саме від Аліси. Наступний приклад ілюструє цей протокол.

Приклад. Припустімо, що Алісин відкритий ключ системи RSA той самий, що й у попередньому прикладі, тобто $n = 53 \cdot 67 = 3551$ і $e = 17$. Її секретний ключ, як знайдено у попередньому прикладі, $d = 1817$. Нехай Алиса хоче передати повідомлення «ЗУСТРІЧ ВІДМІНЕНО». Що саме вона має послати?

Спершу Аліса перекладе повідомлення у блоки цифр й отримає таку послідовність блоків:

0923 2122 2011 2702 1105 1611 1706 1718.

Далі вона застосує **дешифрувальну** функцію $D_{(3551,\,17)}(y) = y^{1817} \bmod 3551$ до кожного блоку. Використовуючи швидке модулярне піднесення до степеня (з використанням комп'ютера) вона знайде, що $0923^{1817} \bmod 3551 = 0445$, $2122^{1817} \bmod 3551 = 1928$, $2011^{1817} \bmod 3551 = 3284$, $2702^{1817} \bmod 3551 = 0953$, $1105^{1817} \bmod 3551 = 3501$, $1611^{1817} \bmod 3551 = 1465$, $1706^{1817} \bmod 3551 = 2188$, $1718^{1817} \bmod 3551 = 3042$.

Отже, лист, розділений на блоки, який надішле Аліса, виглядає так:

0445 1928 5284 0953 3501 1465 2188 3042.

Коли її товариші отримають цей лист, вони застосують її (тобто Алісину) **шифрувальну** функцію (яка відкрита) $E_{(3551,17)}(x) = x^{17} \bmod 3551$ до кожного з цих блоків. Коли вони зроблять це, то отримають блоки цифр оригінального листа, який легко можна перекласти українською мовою. Зокрема, $E_{(3551,17)}(0445) = 0445^{17} \bmod 3551 = 0923$, що при перекладі дасть «ЗУ…» і т. д.

Зазначимо, що в протоколі цифрового підпису головну роль відіграють співвідношення

$$D_{(n,e)}\left(E_{(n,e)}(x)\right) = E_{(n,e)}\left(D_{(n,e)}(x)\right) = x.$$

Ці співвідношення зводяться до рівностей

$$\left(x^e\right)^d \bmod n = \left(x^d\right)^e \bmod n = x,$$

і виражають той факт, що шифрувальна функція $E_{(n,e)}$ і де шифрувальна функція $D_{(n,e)}$ є взаємно оберненими.