КОДУВАННЯ ДАНИХ

У цьому розділі ви отримаєте нові, а також поглибите та розширите свої знання й удосконалите навички з таких тем:

- кодування та декодування повідомлень;
- кодування текстових, графічних і мультимедійних даних;
- таблиці кодів символів;
- колірні моделі;
- двійкове кодування;
- одиниці вимірювання довжини двійкового коду.

1.1. КОДУВАННЯ ТА ДЕКОДУВАННЯ ПОВІДОМЛЕНЬ

У цьому пункті йтиметься про:

- сутність процесу кодування;
- правила для здійснення кодування;
- сутність процесу декодування.

КОДУВАННЯ ПОВІДОМЛЕНЬ

Пригадайте

• Які інформаційні процеси ви знаєте? • Які існують способи подання повідомлень? • Що ви знаєте про шифрування повідомлень? Хто і для чого його використовує? У чому воно полягає?

Під час опрацювання повідомлень, поданих словами, числами, графічними зображеннями, звуками тощо, часто змінюють спосіб подання з метою зберігання, передавання, опрацювання або захисту повідомлень. Наведемо кілька прикладів:

- Усні повідомлення записують на папері, замінюючи звуки людської мови літерами алфавіту. Водночас виконується збереження повідомлень.
- Під час розмови мобільним телефоном звукові сигнали перетворюються на електромагнітні хвилі. Це робить можливим передавання повідомлень на великі відстані.
- Розв'язуючи задачу на уроці математики, числівники записують цифрами, а математичні операції – спеціальними знаками. Це спрощує опрацювання числових даних.
- Для захисту повідомлень від сторонніх осіб здійснюють шифрування, замінюючи літери в тексті повідомлення іншими літерами, числами або іншими умовними позначеннями.

Процес заміни однієї послідовності сигналів, якою подано повідомлення, іншою послідовністю сигналів називають **кодуванням повідомлення.**

Код (лат. *codex* – книга) – система умовних сигналів для передавання, опрацювання та зберігання повідомлень.

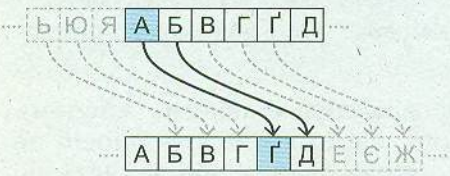
У наш час кодування широко використовують для опрацювання повідомлень не лише людиною, а й цифровими пристроями. Для цього потрібно подати дані у вигляді, придатному для їх опрацювання пристроями.

Мал. 1.1. Штрихкод товару

Наприклад, відомості про товари кодують з використанням штрихкодів (мал. 1.1). Групи цифр на штрихкоді є кодами країни та підприємства, що є виробником певного товару, та самого товару. Людина може проаналізувати цей числовий код, коли купує товар у магазині. Але ті самі відомості кодуються також товщиною ліній штрихкоду та відстанню між ними. Цей графічний код сприймається спеціальними сканерами та опрацьовується з використанням комп'ютера, коли ви оплачуєте товар на касі.

Усі повідомлення – текстові, числові, графічні, звукові та інші, які ми створюємо, зберігаємо та опрацьовуємо з використанням комп'ютера, кодуються з використанням двійкового коду, з яким ви ознайомитеся на наступних уроках.

Для кодування повідомлень визначають не лише набір сигналів, які будуть використані для заміни сигналів заданого повідомлення, а й правила, за якими здійснюється ця заміна.



Мал. 1.2. Правила заміни символів за шифром Цезаря зі зсувом на 4 літери праворуч

Наприклад, з історії добре відомо шифр, яким користувався для секретного листування зі своїми генералами римський імператор Гай Юлій Цезар (100 р. до н. е. – 44 р. до н. е.). Правило кодування полягає в тому, що кожна літера в тексті повідомлення замінюється іншою, що міститься в алфавіті на відстані кількох позицій від заданої літери (мал. 1.2).

Так, закодувавши повідомлення «*привіт*» з використанням шифру Цезаря зі зсувом на 4 літери праворуч, отримуємо повідомлення «*уфкелц*».

Мал. 1.3. Диск для кодування повідомлень за шифром Цезаря

На малюнку 1.3 наведено вигляд диска, який було виготовлено для спрощення процесу кодування повідомлень за шифром Цезаря.

У наш час шифрування широко використовується для захисту повідомлень від несанкціонованого доступу під час їх передавання комп'ютерними мережами.

ДЕКОДУВАННЯ ПОВІДОМЛЕНЬ

Поміркуйте

• Чи може шифрування та розшифрування виконуватися за одними й тими самими правилами? • Що відбудеться, якщо спробувати відкрити графічний файл у програмі **Блокнот**? Із чим це пов'язано?

На основі правила, за яким кодується повідомлення, утворюється правило для відновлення початкового повідомлення. Процес отримання початкового повідомлення із закодованого називають **декодуванням** повідомлення.

Декодування повідомлень відбувається, коли ми читаємо вголос надрукований текст, виконуємо музичний твір по нотах, розшифровуємо повідомлення, визначаємо за штрихкодом країну, у якій виготовлено товар, тощо.

Так, для декодування повідомлення, закодованого шифром Цезаря зі зсувом на 4 літери праворуч, потрібно кожну літеру закодованого повідомлення замінити іншою, що розміщена в алфавіті на 4 позиції ліворуч від заданої. Таким чином, декодувавши повідомлення «*зтдфкн зисб*», отримуємо «*добрий день*».

У комп'ютерних системах файли, у яких зберігаються дані різних типів, є прикладами закодованих повідомлень. Для кодування даних кожного типу (текстових, графічних, звукових тощо) використовують різні алгоритми. Відповідно до використаних алгоритмів кодування утворюються файли різних форматів (**DOCX**, **TXT**, **BMP**, **JPG**, **MP3** та інші).

Коли файл відкривають для опрацювання у відповідній програмі, відбувається процес декодування. Якщо спробувати відкрити файл у невідповідній програмі, то початкове повідомлення не буде відтворено, оскільки така програма не містить потрібного алгоритму декодування.

Кодування та декодування повідомлень є прикладами інформаційних процесів опрацювання даних.

Для тих, хто хоче знати більше

Зрозуміло, що не для кожного закодованого повідомлення передбачається його вільне декодування будь-яким користувачем.

Шифрування – це процес кодування даних, який використовується для захисту вмісту повідомлення від сторонніх осіб і лише визначені користувачі можуть виконати **дешифрування**. Для цього вони повинні знати правило декодування. Таким чином забезпечується конфіденційність даних.

Шифрування передбачає використання криптографічного ключа в поєднанні з різними математичними алгоритмами. **Криптографічний ключ** – це набір даних, як правило, математичних величин, узгоджених між відправником і отримувачем повідомлення.

Шифрування може виконуватися з використанням симетричних або асиметричних алгоритмів.

Криптографія (грец. *κρυπτός* – прихований, *γράφω* – писати) – наука про математичні методи забезпечення захисту інформації.

Симетричний алгоритм шифрування використовує один криптографічний ключ і симетричні правила для шифрування та дешифрування даних. Відомий вам шифр Цезаря є симетричним алгоритмом шифрування. У ньому число, що визначає величину зсуву, є криптографічним ключем. Якщо для шифрування вибрано, наприклад, зсув на 4 літери праворуч, то для дешифрування – зсув на 4 літери ліворуч. Симетричність полягає в тому, що для шифрування та дешифрування величина зсуву однакова, а напрямки протилежні.

Асиметричний алгоритм шифрування, на відміну від симетричного, передбачає використання різних ключів для шифрування та дешифрування даних. Один із цих ключів є **відкритим**, а інший – **закритим**. Використовуючи відкритий ключ, будь-хто може зашифрувати повідомлення, але дешифрувати його може лише той, хто має закритий ключ. У цьому полягає асиметричність алгоритму.

Відкритий і закритий ключі математично пов'язані один з одним. Але, знаючи відкритий ключ, для пошуку закритого ключа, навіть з використанням найпотужніших комп'ютерів, потрібно часу більше, ніж тривалість людського життя.

Одним з популярних алгоритмів асиметричного шифрування є алгоритм **RSA**, який запропонували в 1977 році вчені Массачусетського університету Р. Рівест, А. Шамір і Л. Адлеман. Алгоритм отримав назву від перших літер їх прізвищ (**R**ivest, **S**hamir, **A**dleman). Відповідно до цього алгоритму обирають два різних простих числа, у записі яких понад сто цифр, та знаходять їх добуток. Він є складовою відкритого ключа. Закритий ключ обчислюють на основі одного з обраних простих чисел.

Алгоритм RSA використовують для створення електронних підписів, шифрування каналів мобільного зв'язку, в системах електронної комерції тощо.

Працюємо з комп'ютером

Завдання та алгоритми їх виконання ви зможете знайти за адресою *https://cutt.ly/Je2cOcCZ* або QR-кодом.

Найважливіше в цьому пункті

Кодування повідомлення – це процес заміни однієї послідовності сигналів, якою подано повідомлення, іншою послідовністю сигналів.

Кодування повідомлень виконується з метою їх зберігання, передавання, подальшого опрацювання, захисту. Для кодування повідомлень визначають набір сигналів, які будуть використані для заміни сигналів заданого повідомлення, та правила, за якими здійснюється ця заміна.

Декодування повідомлення – це процес отримання початкового повідомлення із закодованого.

Кодування використовується для опрацювання повідомлень не лише людиною, а й цифровими пристроями. Для цього потрібно подати дані у вигляді, придатному для опрацювання пристроями. У комп'ютерних системах файли, у яких зберігаються дані різних типів, є прикладами закодованих повідомлень. Для кодування даних кожного типу використовують різні алгоритми. Відповідно до використаних алгоритмів кодування утворюються файли різних форматів.

Дайте відповіді на запитання

1. У чому полягає процес кодування повідомлень?
2. З якою метою виконують кодування повідомлень?
3. Що потрібно попередньо визначити для кодування повідомлення?
4. У чому полягає процес декодування повідомлень?
5. Що означає формат файлу, який обирають під час збереження даних у файлі?