Житомирська політехніка	Міністерство освіти і науки України Державний університет «Житомирська політехніка»

ЛЕКЦІЯ №8

ОСНОВИ СТЕГАНОГРАФІЇ. КОДУВАННЯ ІНФОРМАЦІЇ

ПЛАН ЛЕКЦІЇ:

1. ПОНЯТТЯ СТЕГАНОГРАФІЇ. ВИМОГИ ДО СТЕГОСИСТЕМ.

2. СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ.
   - КЛАСИЧНА СТЕГАНОГРАФІЯ
   - КОМП’ЮТЕРНА СТЕГАНОГРАФІЯ

3. ЗАГАЛЬНІ ВІДОМОСТІ ПРО КОДУВАННЯ ІНФОРМАЦІЇ.

4. ЗАГАЛЬНОДОСТУПНІ КОДОВІ СИСТЕМИ.

5. СЕКРЕТНІ КОДОВІ СИСТЕМИ.

ПИТАННЯ №1

ПОНЯТТЯ СТЕГАНОГРАФІЇ. ВИМОГИ ДО СТЕГОСИСТЕМ

ПОНЯТТЯ СТЕГАНОГРАФІЇ

Стеганографія – це метод організації зв’язку, який приховує саму наявність зв’язку.

Слово «стеганографія» у перекладі із грецького буквально означає «тайнопис» (steganos – секрет, таємниця; graphy – запис). Це може бути «невидиме» чорнило, мікрофотознімки, умовне розташування знаків, таємні канали й засобу зв’язку на плаваючих частотах тощо.

Стеганографічна система або ***стегосистема*** – це сукупність засобів і методів, які використовуються для формування схованого каналу передачі інформації.

ПОНЯТТЯ СТЕГАНОГРАФІЇ

При побудові стегосистеми повинні враховуватися наступні положення:

- Супротивник має повне представлення про стеганографічну систему й деталі її реалізації. Єдиною інформацією, яка залишається невідомою потенційному супротивникові, є ключ, за допомогою якого тільки його власник може встановити факт присутності й зміст схованого повідомлення.
- Якщо супротивник якимось чином довідається про факт існування прихованого повідомлення, це не повинно дозволити йому отримати подібні повідомлення в інших даних доки ключ зберігається в таємниці.
- Потенційний супротивник повинен бути позбавлений яких-небудь технічних і інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

УЗАГАЛЬНЕНА МОДЕЛЬ СТЕГОСИСТЕМИ

ПОНЯТТЯ СТЕГАНОГРАФІЇ

Контейнер – це будь-яка інформація, призначена для приховання таємних повідомлень.

Порожній контейнер – контейнер без вбудованого повідомлення; заповнений контейнер або стегоконтейнер, що містить вбудовану інформацію.

Вбудоване (сховане) повідомлення – повідомлення, що вбудовується в контейнер.

Стеганографічний канал або просто ***стегоканал*** – канал передачі стего(стеганограми).

Стегоключ або просто ***ключ*** – секретний ключ, необхідний для приховання інформації. Залежно від кількості рівнів захисту (наприклад, вбудовування у попередньо зашифроване повідомлення) у стегосистемі може бути один або кілька стегоключів.

За аналогією із криптографією, по типу стегоключа стегосистеми можна поділити на два типи: із секретним ключем; із відкритим ключем.

ПОНЯТТЯ СТЕГАНОГРАФІЇ

Будь-яка стегосистема повинна відповідати наступним вимогам:

- Властивості контейнера повинні бути модифіковані, щоб зміну неможливо було виявити при візуальному контролі. Ця вимога визначає якість приховання впроваджуваного повідомлення: для забезпечення безперешкодного проходження стегоповідомлення по каналу зв'язку воно жодним чином не повинне привернути увагу атакуючого.
- Стегоповідомлення повинне бути стійким до викривлень, у тому числі й зловмисних. У процесі передачі зображення (звук або інший контейнер) може піддаватися різним трансформаціям: зменшуватися або збільшуватися, перетворюватися в інший формат тощо. Крім того, воно може бути стиснуте, у тому числі й з використанням алгоритмів стискування із втратою даних.
- Для збереження цілісності, для повідомлення, що вбудовується, необхідно використовувати код з виправленням помилки.
- Для підвищення надійності, повідомлення, що вбудовується, повинне бути продубльовано.

НАПРЯМИ ВИКОРИСТАННЯ СТЕГАНОГРАФІЇ

Стеганографія може використовуватися для різних напрямків, таких як:

- ***Захист від копіювання*** – це напрямок, який пов'язаний з електронною комерцією, контролем за тиражуванням (наприклад, DVD), розповсюдженням мультимедійної інформації (наприклад, відео по запиту). За допомогою стеганографії можна вбудовувати у файл або сигнал спеціальні маркери, які дозволяють ідентифікувати джерело або власника контенту, перевіряти його легальність або виявляти спроби несанкціонованого копіювання. Це також називається цифровим водяним знаком або цифровим печаткою.
- ***Аутентифікація*** – це напрямок, який пов'язаний з системами відеоспостереження, електронної комерції, голосової пошти, електронного конфіденційного діловодства. За допомогою стеганографії можна вбудовувати у файл або сигнал спеціальну інформацію, яка дозволяє підтвердити автентичність або цілісність контенту, перевіряти його джерело або призначення, запобігати підробці або змінам. Це також називається цифровим підписом.
- ***Прихована комунікація*** – це напрямок, який пов'язаний з передачею конфіденційної інформації в небезпечних або обмежених середовищах. За допомогою стеганографії можна вбудовувати у файл або сигнал таємне повідомлення, яке не буде помітне для сторонніх осіб або систем моніторингу. Це дозволяє забезпечити приватність і анонімність комунікації, обходити цензуру або фільтрацію, запобігати перехопленню або блокуванню. Це також називається прихованим каналом.

НАПРЯМИ ВИКОРИСТАННЯ СТЕГАНОГРАФІЇ

- ***Забезпечення конфіденційності***: Одним із основних застосувань стеганографії є збереження конфіденційності інформації. Це може включати в себе приховання корпоративних секретів, особистої інформації або конфіденційних даних від потенційних зловмисників.
- ***Захист від атак***: Стеганографія може використовуватися для приховування даних, що вказують на наявність системних уразливостей або шляхи атаки в інформаційних системах. Це може допомогти уникнути атак і зламу безпеки.
- ***Авторські права***: У галузі мистецтва і медіа стеганографія може використовуватися для захисту авторських прав. Можна приховати водяний знак або інші ідентифікатори в зображеннях або відео, щоб визначити власника контенту.
- ***Контролювання доступу***: Стеганографія може бути використана для керування доступом до різних ресурсів. Наприклад, приховані ключі доступу можуть бути вбудовані в авторизаційні картки або документи.
- ***Боротьба зі злочинністю та тероризмом***: Стеганографія може бути важливим інструментом для правоохоронних органів у виявленні і припиненні злочинної діяльності та терористичних загроз.
- ***Захист від цензури та переслідування***: В країнах, де інтернетова цензура і переслідування є загальною практикою, стеганографія може допомогти користувачам обходити блокування та зберігати свою приватність.
- ***Дослідження та розвідка***: У сфері розвідки і досліджень стеганографія може використовуватися для обміну та приховування секретної інформації між різними сторонами.

СТЕНОГРАФІЧНІ МЕТОДИ

Найпоширеніші методи стеганографії:

- ***Вбудовування в текстовий файл***: Цей метод включає приховання інформації в текстових документах, де букви, регістр і інші параметри тексту можуть бути використані для кодування прихованої інформації. Наприклад, можна вбудовувати приховані повідомлення в пропуски між словами або в незначущі зміни в тексті.
- ***Вбудовування в зображення***: Цей метод використовується для приховування інформації в цифрових зображеннях. Вбудовування в зображення може бути здійснене шляхом зміни кольорів окремих пікселів чи LSB (Least Significant Bit) методом, де найменш значущі біти використовуються для збереження інформації.
- ***Вбудовування в аудіо***: Цей метод полягає в приховуванні інформації в аудіозаписах, зазвичай змінюючи частоту або амплітуду звуку в незначущих областях аудіофайлу.

СТЕНОГРАФІЧНІ МЕТОДИ

- ***Вбудовування в відео***: Вбудовування інформації в відеофайли може бути виконане шляхом модифікації кадрів або звукової доріжки. Цей метод дозволяє приховувати інформацію від переглядачів відео.
- ***Вбудовування в мережевий трафік***: Стеганографія може бути використана для приховування інформації в мережевому трафіку. Це може включати в себе приховану передачу даних через інтернет або інші мережеві протоколи.
- ***Вбудовування в програмний код***: Деякі методи стеганографії включають приховування інформації в програмному коді. Це може відбуватися через вбудовування прихованих коментарів або зашифрованих фрагментів коду.
- ***Використання QR-кодів***: QR-коди, які здаються звичайними зображеннями, також можуть бути використані для приховування текстової або бінарної інформації.

Ці методи можуть використовуватися окремо або в поєднанні для створення більш ефективних методів приховування інформації. Вибір конкретного методу залежить від контексту та завдання, для якого використовується стеганографія.

ЦИФРОВІ ВОДЯНІ ЗНАКИ

Цифрові водяні знаки використовуються для захисту авторських або майнових прав на цифрові зображення, світлини або інші оцифровані твори мистецтва.

Основними вимогами, які висуваються до таких вбудованих даних, є ***надійність*** і ***стійкість до викривлень***.

Цифрові водяні знаки мають невеликий обсяг, однак, з врахуванням вище зазначених вимог, для їх вбудовування використовуються більш складні методи, ніж для вбудовування просто повідомлень або заголовків.

ПИТАННЯ №2

СТЕГАНОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

КЛАСИЧНА СТЕГАНОГРАФІЯ

КЛАСИЧНІ МЕТОДИ СТЕГАНОГРАФІЇ

Серед класичних методів можна виділити такі:

- маніпуляції з носієм інформації (контейнером);
- симпатичне чорнило;
- мікронадписи і мікроточки;
- літературні прийоми;
- семаграми.

МАНІПУЛЯЦІЇ З НОСІЄМ ІНФОРМАЦІЇ

Перші сліди застосування стеганографічних методів губляться в глибокій давнині. Існує версія, що стародавні шумери одними з перших використовували стеганографію, тому що було знайдено безліч глиняних клинописних табличок, у яких один запис покривали шаром глини, а на другому шарі писали інший. Однак противники цієї версії вважають, що це було зовсім не спробою приховування інформації, а всього лише практичною потребою.

МАНІПУЛЯЦІЇ З НОСІЄМ ІНФОРМАЦІЇ

У третій і сьомій книгах "Історії" давньогрецького вченого Геродота зустрічається опис ще двох методів приховування інформації:

- у V столітті до н.е. грецький тиран Гістій, перебуваючи під наглядом перського царя Дарія в Сузах, мав послати секретне повідомлення своєму родичу в анатолійське місто Мілет. Він поголив наголо свого раба і витатуював послання на його голові. Коли волосся знову відросло, раба відправили в дорогу;
- у Стародавній Греції тексти писали на дощечках, покритих воском. У 480 р. до н.е. перська армія під проводом Ксеркса I рухалася на грецькі міста-держави. Дізнавшись, що Ксеркс готовий до виступу, грецький цар Демарат, засланий до Персії, попередив про це спартанців. Він зішкрябав віск із двох дерев'яних дощечок для письма, написав усе, що йому стало відомо про наміри персів, а потім знову покрив дощечки воском. Ці на вигляд чисті дощечки були без проблем доставлені в Лакедемон (Спарта). Горго, дружина царя Леоніда, уважно оглянула дощечки і виявила приховане послання. Те, що вона прочитала, принесло їй і радість, і горе. Її чоловік, Леонід, зі своїми людьми поспішив форсованим маршем до вирішального рубежу оборони на шляху наступаючих персів. Цим місцем був прохід, що називався Фермопіли. Через зрадників, які знали таємний шлях, Леонід і його 300 воїнів-спартанців загинули, але вони три дні утримували свої позиції, давши час містам-державам підготуватися до бою і здобувши славу героїв.

МАНІПУЛЯЦІЇ З НОСІЄМ ІНФОРМАЦІЇ

Еней Тактик у своїх історичних трактатах (IV ст. до н.е.) описував спосіб таємного передавання послань, коли в пергаменті над або під написаними літерами проколювали крихітні отвори. Цим способом користувалися в Англії до появи телеграфу з метою уникнути великих витрат на поштову пересилку. Відправлення листів на далекі відстані коштувало вкрай дорого, старі ж газети з наклеєною маркою можна було пересилати країною взад і вперед. Багато хто з тих, хто не в змозі був дозволити собі оплатити поштові витрати, ставили в газетах крапки над буквами; таким чином, вони писали листи, які потім доставляли безкоштовно. Одержувач просто послідовно виписував усі позначені таким чином літери, і в результаті виходило адресоване йому повідомлення.

До 1000 р. н.е. китайські воєначальники записували важливі повідомлення на дуже тонкому папері або шовку. Потім таке послання щільно скочувалося і покривалося воском. Коли віск вистигав, кур'єр ховав лист у своєму одязі, проковтував або користувався як схованкою одним із отворів власного тіла.

МАНІПУЛЯЦІЇ З НОСІЄМ ІНФОРМАЦІЇ

Класичний приклад фізичного приховування інформації – люлька для паління, настільки улюблена секретними агентами. Повідомлення ховали в порожнині стінок чаші і прикривали внутрішньою (поворотною) частиною чаші, водночас можна було, набивши трубку тютюном, курити її. У разі небезпеки шпигунові достатньо було злегка повернути внутрішню частину чаші, щоб папір із записаним на ньому повідомленням упав у палаючий тютюн.

Наведемо цікавий хімічний спосіб запису секретних повідомлень усередині вареного яйця. Береться суміш галуну, чорнила й оцту, записується нею на шкаралупі послання, витримується в міцному розсолі або оцті, щоб стравити з поверхні сліди, і вариться яйце круто. У результаті текст повідомлення опиняється під шкаралупою зверху білка.

СИМПАТИЧНЕ ЧОРНИЛО

Симпатичне (невидиме) чорнило – чорнило, записи яким є від самого початку невидимими і стають видимими тільки за певних умов (нагрівання, освітлення, хімічний проявник тощо).

Невидимим чорнилом користувалися ще за часів Римської імперії. У I ст. н.е. римський письменник Пліній Старший у своїй "Природничій історії" описував застосування для тайнопису рідини, виготовленої з молочаю. Грецький військовий учений Філон Візантійський писав про рідину з чорнильних горішків, завдяки якій написане повідомлення було невидимим. Арабські вчені на початку XV ст. згадували про деякі суміші з рослин, які росли в їхньому регіоні; те саме стосувалося таких письменників епохи Відродження, як Леон Баттіста Альберті та Джованні Порта. Французький сатирик Франсуа Рабле в романі "Ґаргантюа і Пантаґрюель" (1532 р.) з гумором розмірковував про тайнопис. Серед інших дотепних коментарів про життя він описував спосіб приготування невидимого чорнила з таких речовин, як сік білої цибулі, нашатир і галун.

СИМПАТИЧНЕ ЧОРНИЛО

Прикладом може слугувати цікавий історичний епізод: повсталі дворяни в Бордо заарештували францисканського ченця Берто, який був агентом кардинала Мазаріні. Повсталі дозволили Берто написати листа знайомому священику в місто Блей. Однак наприкінці цього листа релігійного змісту, монах зробив приписку, на яку ніхто не звернув увагу: "Посилаю Вам очну мазь; натріть нею очі і Ви будете краще бачити". Так він зумів переслати не тільки приховане повідомлення, а й вказав спосіб його виявлення. У результаті ченець Берто був врятований.

Симпатичне чорнило буває, як правило, двох видів: хімічне та органічне. Перші являють собою хімічні розчини, які робляться невидимими при висиханні. Приховані слова стають видимими під час додавання до них інших хімічних препаратів, званих реагентами. Органічна група представлена здебільшого легкодоступними речовинами, такими, як цибуля, лимон, молоко та оцет. Вони зазвичай стають видимими, якщо їх обережно нагріти.

СИМПАТИЧНІ ЧОРНИЛА ТА ЇХНІ ПРОЯВНИКИ

Чорнило	Проявник
Лимонна кислота (харчова)	Бензилоранж
Віск	CaCOз або зубний порошок
Яблучний сік	Нагрівання
Молоко	Нагрівання
Сік цибулі	Нагрівання
Сік брукви	Нагрівання
Пірамідон (у спиртовому розчині)	Нагрівання
В'яжучі засоби для дезінфекції рота і глотки	Нагрівання
Галун	Нагрівання
Слина	Дуже слабкий водний розчин чорнила
Фенолфталеїн	Розбавлений луг
Пральний порошок	Світло лампи ультрафіолету
Крохмаль	Йодна настоянка
Аспірин	Солі заліза

СИМПАТИЧНЕ ЧОРНИЛО

З метою виявлення таємних повідомлень, написаних за допомогою симпатичного чорнила, американські цензори під час Другої світової війни "полосовали" листи, щоб виявити наявність у них невидимого чорнила. Лаборант водив по листу кількома щітками, закріпленими в одному тримачі і змоченими в розчинах різних проявників. Ці проявники мали різні властивості і реагували навіть на виділення людини, тож після обробки на папері з'являлися відбитки пальців і краплі поту.

Листи також проходили перевірку в інфрачервоних і ультрафіолетових променях. Текст, написаний крохмалем і невидимий при денному або електричному світлі, починав світитися під впливом ультрафіолету. Інфрачервоні промені допомагали розрізняти кольори, які неможливо розрізнити при звичайному освітленні. Наприклад, зелені написи на зеленій поштовій марці.

Проблеми, у яких місцеві відділення не могли розібратися своїми силами, передавали в лабораторію відділу безпеки. Одна з таких проблем полягала в тому, що німецькі агенти розшаровували аркуш паперу навпіл, писали текст невидимим чорнилом на внутрішній поверхні, а половинки потім знову з'єднували між собою. Оскільки чорнило опинялося всередині аркуша, жоден реагент, нанесений на його зовнішню поверхню, не міг його проявити. Цей виверт було виявлено лише після того, як один німецький агент використав для свого письма занадто багато чорнила і його надлишок просочився крізь папір.

СИМПАТИЧНЕ ЧОРНИЛО

У 2011 р. Мануель Паласіос (Manuel Palacios) з університету Тафтса та Джордж Вайтсайдс (George Whitesides) з Гарварду спробували заховати повідомлення в масиві, що складається з семи штамів **бактерій** Escherichia coli (E. coli). Техніку жартома назвали **SPAM** (Steganography by Printed Arrays of Microbes), що можна перекласти як стеганографія за допомогою друкованих масивів мікробів.

Вчені створили сім штамів бактерій, кожен з яких виробляє свій білок, що флуоресціює при певному світлі (подробиці – у статті в журналі PNAS). Колонії бактерій наносяться на підкладку у вигляді рядів точок. Кожна пара точок (кольорів) є кодом для букви, цифри або символу. Сім кольорів дають 49 комбінацій, автори роботи використовували їх для кодування 26 літер і 23 інших символів (таких як, цифри, @ або $). Наприклад, дві жовті крапки позначають букву "t", а комбінація помаранчевої та зеленої – "d". Одержувач, знаючи коди дешифрування, легко прочитає надіслане повідомлення - світіння помітне неозброєним оком.

ПРИКЛАД "ПРОЯВЛЕНОГО" ПОСЛАННЯ

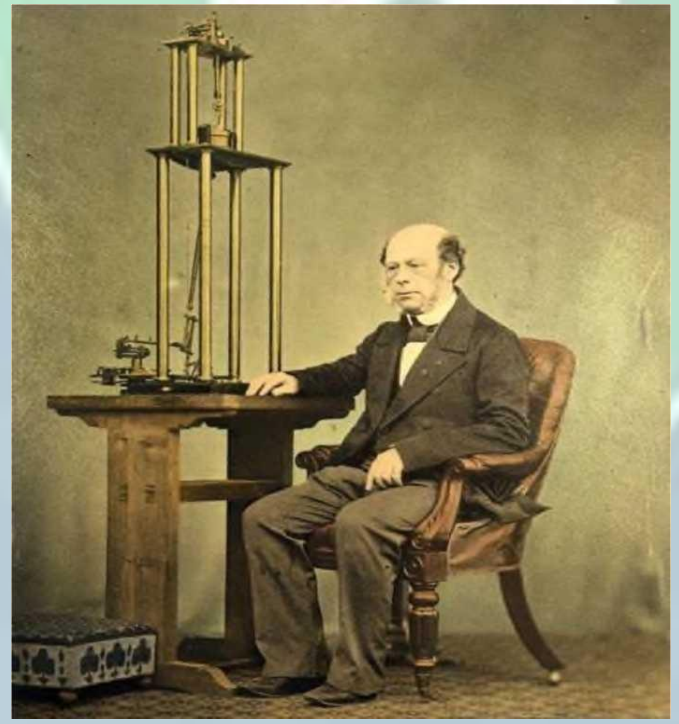
СИМПАТИЧНЕ ЧОРНИЛО

Щоб створити повідомлення, біологи наносять штами E.coli, стійкі до певного антибіотика, на підкладку з агаром (середовищем, поживним для бактерій). Потім поверх підкладки кладуть аркуш із нітроцелюлози – колонії друкуються на ньому. Для проявлення повідомлення одержувач повинен буде помістити нітроцелюлозний аркуш у чашку з "проявочним" агаровим середовищем, що запускає роботу потрібних генів і світіння штамів. До складу "проявного" агарового середовища входить правильний антибіотик, який вбиває всі мікроорганізми, крім тих, що кодують повідомлення (адже вони стійкі до дії ліків). У результаті під час проявлення він отримає потрібний код.

Наразі британські та американські дослідники пробують подібним чином зашифрувати повідомлення за допомогою дріжджів і спороносних бактерій, а надалі "зазіхають" і на рослини. "Було б чудово заховати інформацію у формі листя або малюнку кореневої системи. Чим більше рис, тим більший обсяг даних можна зашифрувати", – каже Паласіос.

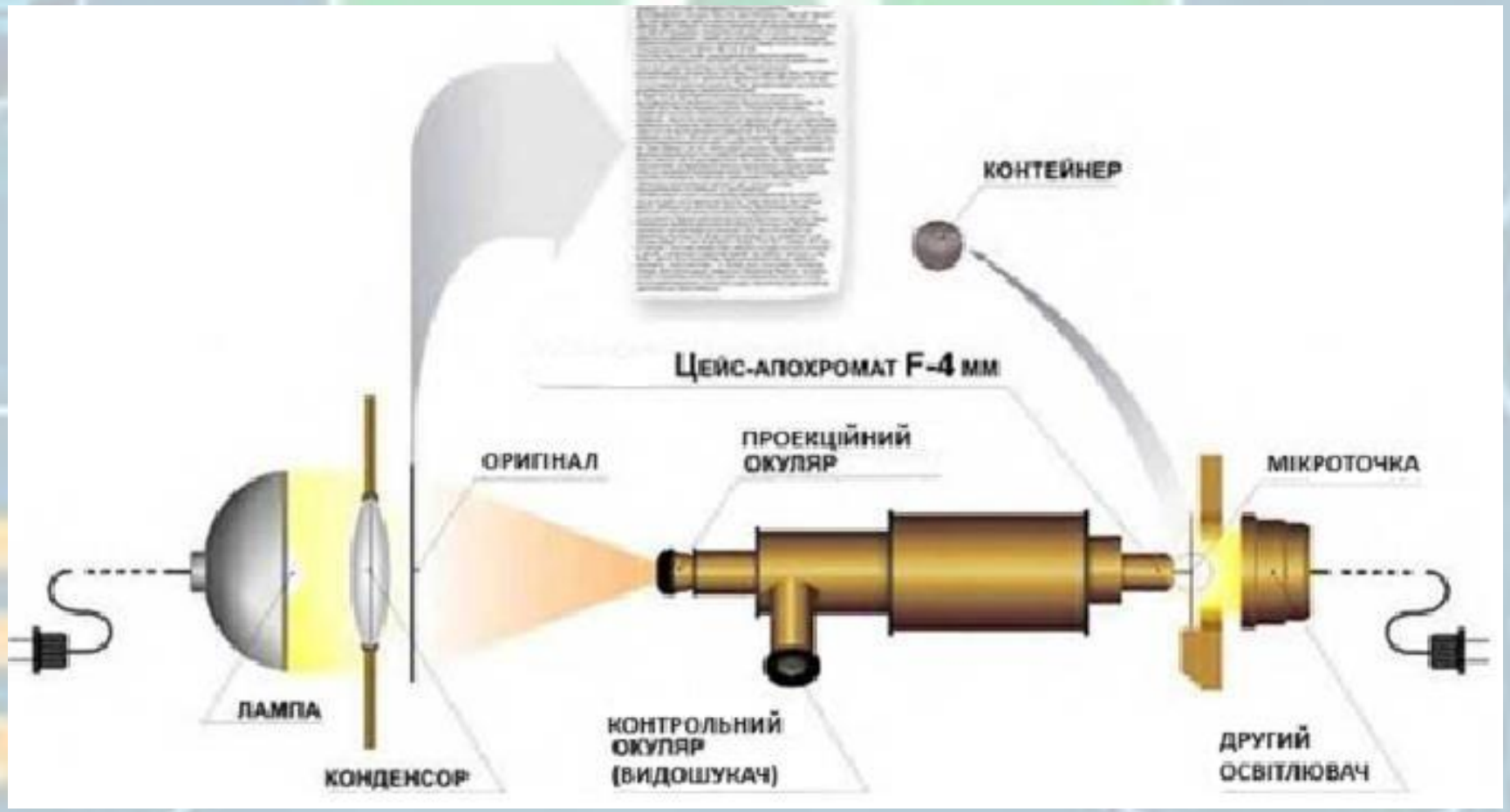
МІКРОНАДПИСИ І МІКРОТОЧКИ

Уже в XVIII столітті в Англії та Франції було створено спеціальні механічні пристрої для виконання мікронадписів. Один із найдосконаліших таких пристроїв, Peter's Machine for Microscopic Writing (1862 р.), зберігається в музеї Оксфордського університету. Він давав змогу виконувати написи з висотою символів усього у 2,5 мікрона. Машина Петра для мікроскопічного письма:



МІКРОНАДПИСИ І МІКРОТОЧКИ

Першим творцем "справжньої" мікроточки історики справедливо вважають Еммануїла Голдберга, який у 1925 р. не тільки зібрав оригінальну оптичну схему для її фотографування, а й докладно описав усі етапи створення фото з високою роздільною здатністю. Оптична схема Голдберга для виготовлення мікроточки:



МІКРОНАДПИСИ І МІКРОТОЧКИ

З англійських і американських архівів випливає, що німецька розвідка АБВЕР перед Другою світовою війною найактивнішим чином використовувала мікроточки для зв'язку з агентурою в Північній і Латинській Америці. За словами Гувера, перше попередження про існування мікроточок ФБР отримало в січні 1940 р. Але виявили таку мікроточку лише в серпні 1941 р., коли якийсь технік-фотолаборант випадково помітив відблиск світла на конверті, вилученому в німецького агента, який потрапив під підозру. Причиною відблиску стала мікрокрапка, замаскована під крапку наприкінці речення.

Західні історики мікрофотографії також стверджують, що і радянська розвідка використовувала мікроточки ще до початку війни. Після закінчення війни в 1945 р. мікроточки широко застосовували радянські агенти, які діяли по всьому світу. Одним із таких агентів був Рудольф Абель. Він використовував цей метод у 1950-х рр., займаючись шпигунською діяльністю в районі Нью-Йорка.

Мікроточки мали здатність передавати великі обсяги інформації (сотні сторінок і креслень в одній точці) і зазвичай вклеювалися в лист або книгу. Мікроточки ховали в прикрасах, монетах, батарейках, предметах побуту, поміщали в надрізаний край листівки з подальшим акуратним заклеюванням надрізу.

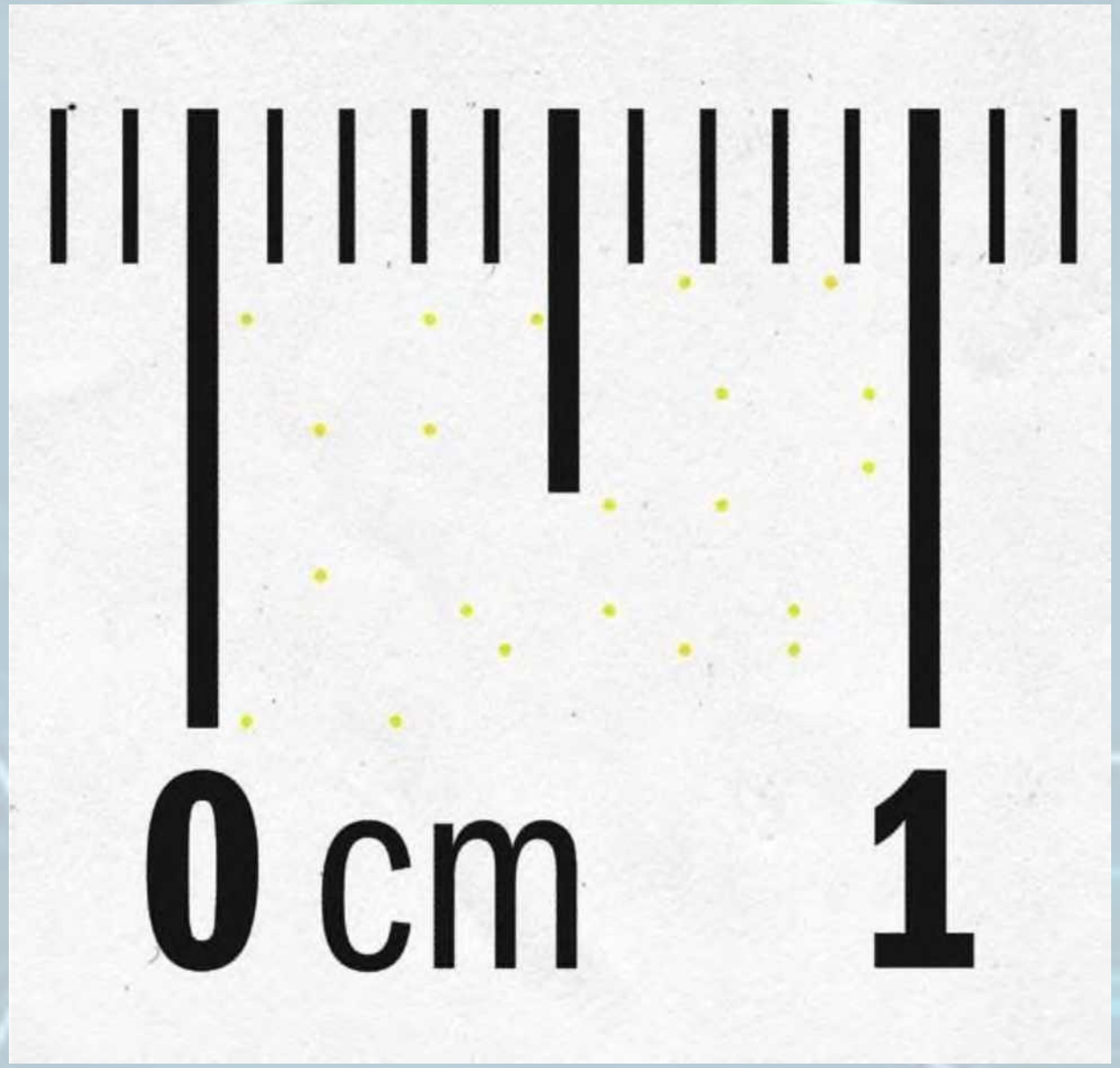
МІКРОНАДПИСИ І МІКРОТОЧКИ

У 2001 р. в Австралії було розроблено технологію нанесення мікроточок, що містять Персональний ідентифікаційний номер (ПІН), на найважливіші деталі виробу (зазвичай – автомобіля). Такі, виготовлені за допомогою лазера прозорі мікроточки наклеюються в непримітних місцях безпосередньо на складальному конвеєрі. Побачити їх можна тільки при освітленні ультрафіолетовим світлом. Цей процес, дешевий і ефективний, ускладнює викрадачам автомобілів легальний продаж викраденої та розібраної машини у вигляді "запчастин".

Виробники кольорових принтерів додавали в них функцію друку так званих "жовтих точок".

Ці точки, ледь помітні неозброєним оком, друкувалися на кожній сторінці та містили в собі інформацію про серійний номер принтера, а також дату і час друку. Підтверджено використання цього методу в принтерах, що випускаються під торговими марками Brother, Canon, Dell, Epson, Hewlett-Packard, IBM, Konica, Kyocera, Lanier, Lexmark, NRG, Panasonic, Ricoh, Savin, Toshiba, Xerox. Введення цього заходу, згідно з коментарями виробників, було частиною співпраці з урядом і консорціумом банків, спрямованого на боротьбу з фальшивомонетниками.

ЖОВТІ ТОЧКИ



МІКРОНАДПИСИ І МІКРОТОЧКИ

Екзотичним способом зберігання і передачі інформації є використання для цих цілей ДНК-молекул. У клітинах тварин і рослин **ДНК** (дезоксирибонуклеїнова кислота) міститься в ядрі клітини у складі хромосом, а також у деяких клітинних органелах (мітохондріях і пластидах). У клітинах бактерій молекулаДНК прикріплена зсередини до клітинної мембрани. У них і в нижчих еукаріотів (наприклад, дріжджів) трапляються невеликі автономні молекули ДНК, звані плазмідами. Крім того, ДНК-молекули можуть утворювати геном деяких вірусів.

У 1998 р. бразильський художник Едуардо Кац переклав фразу з Книги Буття (лат. Genesis) у код Морзе, який, у свою чергу, представив у вигляді послідовності ДНК. Цитату з Буття, заради експерименту, трохи скоротили і модифікували: "І нехай панує людина над рибами морськими, і над птахами небесними, і над усякою живністю, яка рухається по землі" (Let man have dominion over the fish of the sea, and over the fowl of the air, and over every living thing that moves upon the earth). Синтезований ген Кац клонував у плазміди, які потім вмонтував у клітини бактерії E. Coli.

ІНСТАЛЯЦІЯ GENESIS

(ліворуч – цитата у вигляді ДНК; у центрі – проекція чашки Петрі з бактеріями; праворуч – цитата англійською мовою)

МІКРОНАДПИСИ І МІКРОТОЧКИ

ДНК-молекули є компактним і надійним носієм інформації. Група вчених Гарварду підрахувала, що пам'ять зі структур ДНК вагою всього 4 грами теоретично може зберігати всю інформацію, яку виробляє все людство сучасності за один рік. На користь надійності говорить той факт, що інформація з ДНК може бути зчитана через сотні тисяч і навіть мільйони років. "ДНК можна зберігати в далеко не ідеальних умовах – наприклад, у мертвих тварин. При цьому вона збережеться, і через 400 тис. років ми все ще здатні її зчитувати, – розповідає керівник досліджень професор Джордж Черч (George Church) з Гарвардської медичної школи (США). Запис у ДНК зберігатиметься куди довше, ніж на диску Blu-ray".

Для кодування інформації вчені з Гарварду використовували спеціальний струменевий принтер, який поміщає короткі фрагменти хімічно синтезованої ДНК на поверхню крихітного скляного чіпа. Імітуючи двійковий код, дослідники використовували A (аденін) і C (цитозин) як 0, а G (гуанін) і T (тимін) – як 1. Генетичний код використовували, щоб записати вміст книги Дж. Черча "Регенезис. Як синтетична біологія заново придумає природу і нас" ("Regenesis: How Synthetic Biology Will Reinvent Nature And Ourselves"), що складається з 53 тис. слів і 11 зображень (« 300 сторінок). 70 млрд. копій книги було "надруковано" на ДНК-чипі, що приблизно дорівнює нігтю мізинця.

ЛІТЕРАТУРНІ ПРИЙОМИ

Добре відомі різного роду літературні прийоми, призначені для приховування таємної інформації в зовні нешкідливих посланнях.

Пустишковий шифр. При використанні даного шифру (точніше методу) слова або букви секретного повідомлення записуються в певних позиціях. Наприклад, читають кожне п'яте слово або першу букву кожного слова, тоді як всі інші букви або слова слугують як "пустушки" для приховування значущого тексту.

Акровірш. Таємне послання складається з перших букв рядків віршів. Заведено вважати, що акровірш уперше застосував відомий давньогрецький комедіограф, філософ і лікар Епіхарм Сіракузький (V ст. до н.е.). Спочатку функцією акровірша була фіксація імені автора в тексті його твору. Потім ця функція розширилася, у них почали передавати приховані послання, моралі тощо.

Решітка Кардано. Решітка, запропонована Кардано, була картонним або дерев'яним трафаретом, у якому через неправильні інтервали зроблені прямокутні вирізи. Накладаючи цей трафарет на аркуш паперу, можна було записувати у вирізи секретне повідомлення (букву, склад або ціле слово). Після цього починалася тяжка робота з вигадування правдоподібних і нешкідливих на вигляд послань.

Алюзія (лат. allusio – жарт, натяк) або **жаргонний код**. Цей літературний прийом полягає у використанні фраз, які передбачаються відомими тому, до кого звернено мову, і невідомими стороннім особам. Знамениті фрази, які передали по радіо, – "Над усією Іспанією чисте небо" (сигнал до початку франкістського путчу в Іспанії, 17 липня 1936 р.) і "У Сантьяго йде дощ" (сигнал до початку військового перевороту в Чилі, 11 вересня 1973 р.).

ЛІТЕРАТУРНІ ПРИЙОМИ

Семаграма (грец. sema – знак і gramma – написаний, намальований) – таємне повідомлення, у якому секретними кодозамінами є будь-які символи, окрім літер і цифр.

Секретними кодозамінами можуть бути:

- точки на кісточках доміно;
- предмети на фотографії, розташовані таким чином, щоб передати заздалегідь обумовлений сенс;
- вишиті на сукні візерунки, що являють собою закодоване послання;
- картина, на якій довгі й короткі гілки дерев представляють крапки й тире азбуки Морзе;
- тощо.

Одного разу в нью-йоркському цензорному відділенні перевели всі стрілки в призначеній для відправки партії годинників, побоюючись, що їхнє положення може містити в собі якесь повідомлення.

Під час Другої світової війни був зареєстрований випадок, коли німецькі агенти в Англії надіслали в Німеччину своє повідомлення під виглядом зв'язаного светра. Він нібито призначався для ув'язненого, але замість цього потрапив до контррозвідників. Коли светр розпустили, виявилося, що його вовняні нитки були суцільно у вузликах. Пряжу розправили, а вузли зіставили з алфавітом, написаним вертикально на стіні. Базисною лінією було обрано підлогу, а алфавіт розташовувався перпендикулярно до неї.

КОМП’ЮТЕРНА СТЕГАНОГРАФІЯ

ЗАВДАННЯ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

Розвиток комп'ютерної технології та засобів комунікації надали нового імпульсу розвитку та вдосконаленню стеганографії. Сьогодні кожен може скористатися тими перевагами, які дає стеганографія як у сфері прихованого передавання інформації, що особливо корисно в країнах, де існує заборона на стійкі засоби криптографії, так і в сфері захисту авторських прав. Нині методи комп'ютерної стеганографії активно використовують для вирішення таких завдань:

1. **Захист конфіденційної інформації від несанкціонованого доступу**. Ця галузь використання комп'ютерної стеганографії є найефективнішою під час розв'язання проблем захисту конфіденційної інформації. Так, наприклад, обсяг секретного повідомлення у звукових і графічних файлах може становити до 25-30 % від розміру файлу. Причому аудіовізуальні зміни такі, що не виявляються під час прослуховування та перегляду файлів більшістю людей, навіть якщо факт приховування відомий.
2. **Подолання систем моніторингу та управління мережевими ресурсами**. Стеганографічні методи дають змогу протистояти спробам контролю над інформаційним простором під час проходження інформації через сервери управління локальних і глобальних обчислювальних мереж.

ЗАВДАННЯ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

3. **Камуфлювання програмного забезпечення**. Застосовується в тих випадках, коли використання ПЗ незареєстрованими користувачами є небажаним. ПЗ може бути закамуфльоване під стандартні універсальні програмні продукти (наприклад, текстові редактори) або сховане у файлах мультимедіа і використовуватися тільки особами, які мають на це права.
4. **Захист авторських прав**. Одним із найперспективніших напрямків комп'ютерної стеганографії є технологія використання цифрових водяних знаків ЦВЗ (digital watermarking) – у цьому разі створення невидимих оку знаків захисту авторських прав на графічні та аудіо файли. Такі ЦВЗ, поміщені у файл, можуть бути розпізнані спеціальними програмами, які витягнуть з файлу багато корисної інформації: коли створено файл, хто володіє авторськими правами, як вступити в контакт з автором тощо. За тієї повальної крадіжки, яка відбувається в Інтернеті, користь від такої технології очевидна.

Сьогодні на ринку існує досить багато фірм, що пропонують продукти для створення та детектування водяних знаків. Один із лідерів – фірма Digimarc. Її продуктами, якщо вірити наданій самою фірмою інформації, користуються понад мільйон офіційних клієнтів: дизайнери, художники, онлайнові галереї. Спеціальні пошукові агенти сканують ресурси Інтернет, переглядаючи картинки на наявність ЦВЗ, і повідомляють власників про факти використання їхньої власності.

МЕТОДИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

Стеганографічні методи	Коротка характеристика методів	Примітки
1. Методи, засновані на використанні спеціальних властивостей носіїв даних		
1.1 Приховування інформації в невикористовуваних місцях дисків	1 Використовуються доріжки, доступні для читання, але не сприймаються ОС (наприклад, у резервну область жорсткого диска). 2. Запис у невикористовувані місця оптичних дисків (CD, DVD, Blue-ray тощо).	1. Низький ступінь скритності. 2. Можливе передавання великих обсягів інформації.
1.2 Нанесення додаткових доріжок на гнучкі магнітні диски (вийшли з ужитку)	Оскільки ширина доріжки в кілька разів менша за відстань між доріжками (для гнучких магнітних дисків), то на диск можна нанести додаткові доріжки і записати туди інформацію, не доступну ОС.	Можливе передавання великих обсягів інформації.
1.3 Спеціальне форматування дисків	Форматування диска під розмір секторів відмінний від прийнятого в ОС.	1. Наявність програм як тих, що форматують подібним чином диски, так і тих, що читають будь-яке форматування. 2. Можливе передавання великих обсягів інформації.

МЕТОДИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

Стеганографічні методи	Коротка характеристика методів	Примітки
2. Методи, засновані на використанні спеціальних властивостей форматів даних		
2.1 Методи використання полів даних, зарезервованих для розширення	Поля розширення є в багатьох мультимедійних форматах. Вони заповнюються нульовою інформацією і не враховуються програмою.	1. Низький ступінь скритності. 2. Передача невеликих обсягів інформації.
2.2 Методи спеціального форматування в текстових документах	1 Використання зміщення символів, слів, речень або абзаців у тексті (можна забезпечити вставкою додаткових пробілів). 2. Вибір певних позицій символів (наприклад, акростих). 3. Використання додаткових можливостей форматування текстів (наприклад, використання в MS Word: прихованого тексту; спеціальних шрифтів; символів певного шрифту, розміру або кольору; білого кольору для символів і фону; одного пробілу між словами для кодування "0" і двох - для кодування "1" тощо).	1. Слабка продуктивність методів. 2. Передача невеликих обсягів інформації. 3. Низький ступінь скритності.

МЕТОДИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

Стеганографічні методи	Коротка характеристика методів	Примітки
2. Методи, засновані на використанні спеціальних властивостей форматів даних		
2.3 Методи спеціального форматування текстів під час друку	1. Друк спеціальними шрифтами, символами певного шрифту, розміру або кольору. 2. Внесення малопомітних спотворень інформації під час друку (Був використаний під час друку контрактів із клієнтами в одній із московських компаній. Цей тайнопис мав вигляд звичайних незначних дефектів друку і забезпечував певний ступінь підтвердження автентичності документа).	1. Слабка продуктивність методів. 2. Передача невеликих обсягів інформації.
2.4 Приховування інформації у вільних областях диска	1 Використання вільної частини останнього кластера файлу. 2. Використання вільних кластерів без запису в таблиці розміщення файлів інформації про те, що в цих кластерах міститься інформація.	1. Низький ступінь скритності. 2. Можливе передавання великих обсягів інформації.
2.5 Використання особливостей файлової системи	1. використання прихованих файлів. 2. Використання потоків у NTFS.	1. Низький ступінь скритності. 2. Можливе передавання великих обсягів інформації.

МЕТОДИ КОМП'ЮТЕРНОЇ СТЕГАНОГРАФІЇ

Стеганографічні методи	Коротка характеристика методів	Примітки
3. методи, засновані на використанні надмірності аудіо- та відеоінформації		
3.1 Методи використання надмірності мультимедійних форматів	Молодші розряди байт, що несуть інформацію про інтенсивність світла і звуку, містять дуже мало корисної інформації. Їх заповнення практично не впливає на якість сприйняття.	1. За рахунок введення додаткової інформації спотворюються статистичні характеристики цифрових потоків. 2. Для зниження компрометувальних ознак потрібна корекція статистичних характеристик. 3. Можливе передавання великих обсягів інформації.

ПИТАННЯ №3

ЗАГАЛЬНІ ВІДОМОСТІ ПРО КОДУВАННЯ ІНФОРМАЦІЇ

ПОНЯТТЯ КОДУВАННЯ

Кодування – подання інформації в альтернативному вигляді.

За своєю суттю кодові системи (або просто коди) аналогічні шифрам однозначної заміни, у яких елементам кодованої інформації відповідають кодові позначення. **Відмінність полягає в тому**, що в шифрах присутня змінна частина (ключ), яка для певного вихідного повідомлення за одного й того самого алгоритму шифрування може видавати різні шифротексти. ***У кодових системах змінної частини немає***. Тому одне й те саме вихідне повідомлення під час кодування, як правило, завжди має однаковий вигляд. Іншою відмінною особливістю кодування є ***застосування кодових позначень (замін) цілком для слів, фраз або чисел (сукупності цифр)***. Заміна елементів кодованої інформації кодовими позначеннями може бути виконана на основі відповідної таблиці (на кшталт таблиці шифрозамін) або визначена за допомогою функції чи алгоритму кодування.

ЕЛЕМЕНТИ ІНФОРМАЦІЇ, ЩО КОДУЄТЬСЯ

Як елементи інформації, що кодується, можуть виступати:

- букви, слова і фрази природної мови;
- різні символи, такі як розділові знаки, арифметичні та логічні операції, оператори порівняння тощо. Слід зазначити, що самі знаки операцій та оператори порівняння – це кодові позначення;
- числа;
- аудіовізуальні образи;
- ситуації та явища;
- спадкова інформація;
- тощо.

КОДОВІ ПОЗНАЧЕННЯ

Кодові позначення можуть являти собою:

- літери та поєднання букв природної мови;
- числа;
- графічні позначення;
- електромагнітні імпульси;
- світлові та звукові сигнали;
- набір і поєднання хімічних молекул;
- і т.д.

МЕТА КОДУВАННЯ

Кодування може виконуватися з метою:

- зручності зберігання, опрацювання та передавання інформації (зазвичай закодована інформація подається компактніше, а також придатна для опрацювання та передавання автоматичними програмно-технічними засобами);
- зручності інформаційного обміну між суб'єктами;
- наочності відображення;
- ідентифікації об'єктів і суб'єктів;
- приховування секретної інформації;
- тощо.

ВИДИ КОДУВАННЯ ІНФОРМАЦІЇ

Кодування інформації буває **одно-** і **багаторівневим**. ***Прикладом однорівневого кодування*** слугують світлові сигнали, які подає світлофор (червоний – стій, жовтий – приготуватися, зелений – уперед). ***Як багаторівневе кодування можна навести*** подання візуального (графічного) образу у вигляді файлу фотографії. Спочатку візуальна картинка розбивається на складові елементарні елементи (пікселі), тобто кожна окрема частина візуальної картинки кодується елементарним елементом. Кожен елемент подається (кодується) у вигляді набору елементарних кольорів (RGB: англ. red – червоний, green – зелений, blue – синій) відповідною інтенсивністю, яка зі свого боку подається у вигляді числового значення. Згодом набори чисел, як правило, перетворюються (кодуються) з метою більш компактного представлення інформації (наприклад, у форматах jpeg, png тощо). І нарешті, підсумкові числа подаються (кодуються) у вигляді електромагнітних сигналів для передавання каналами зв'язку або областей на носії інформації. Слід зазначити, що самі числа під час програмного опрацювання подаються відповідно до прийнятої системи кодування чисел.

ВИДИ КОДУВАННЯ ІНФОРМАЦІЇ

Кодування інформації може бути **оборотним** і **необоротним**. При ***оборотному кодуванні*** на основі закодованого повідомлення можна однозначно (без втрати якості) відновити кодоване повідомлення (вихідний образ). Наприклад, кодування за допомогою азбуки Морзе або штрихкоду. За ***необоротного кодування*** однозначне відновлення вихідного образу неможливе. Наприклад, кодування аудіовізуальної інформації (формати jpg, mp3 або avi) або хешування.

ВИДИ СИСТЕМ КОДУВАННЯ ІНФОРМАЦІЇ

Розрізняють **загальнодоступні** и **секретні системи кодування**. Перші використовують для полегшення інформаційного обміну, другі – з метою приховування інформації від сторонніх осіб.

У деяких секретних кодових системах присутні елементи, що дають змогу отримувати різні закодовані повідомлення для певного вихідного повідомлення (адитивні числа, багатозначні заміни, правила перешифрування).

ПИТАННЯ №4

ЗАГАЛЬНОДОСТУПНІ КОДОВІ СИСТЕМИ

ЗАГАЛЬНОДОСТУПНІ КОДОВІ СИСТЕМИ

Кодування інформації знайшло широке застосування в суспільному житті. Як зазначалося вище, навіть самі знаки арифметичних і логічних операцій – це кодові позначення. Зокрема, знак "+" для операції додавання (а також знак "-") придумали в німецькій математичній школі "косистів" (тобто алгебраїстів). Вони використовуються в "Арифметиці" Йоганна Відмана, виданій у 1489 р. До цього додавання позначалося буквою p (plus) або латинським словом et (сполучник "і"), а віднімання – буквою m (minus). У Відмана символ плюса замінює не тільки додавання, а й союз "і". Якщо "копати ще глибше", то буква "А" – це кодове позначення для відповідного звуку.

Як інші поширені кодові системи можна навести інші поширені кодові системи:

- дорожні знаки;
- позначення хімічних елементів із періодичної таблиці Менделєєва;
- знаки зодіаку;
- скорочені найменування дисциплін у розкладі занять студентів.

Далі розглянемо інші загальнодоступні кодові системи з метою ілюстрації різноманіття їхнього призначення та способів подання кодових позначень.

АЗБУКА МОРЗЕ

Азбука Морзе – спосіб кодування символів (літер алфавіту, цифр, розділових знаків тощо) за допомогою послідовності "крапок" і "тире". За одиницю часу приймається тривалість однієї крапки. Тривалість тире дорівнює трьом крапкам. Пауза між елементами одного знака – одна крапка (близько 1/25 частки секунди), між знаками в слові – 3 крапки, між словами – 7 крапок. Названий на честь американського винахідника і художника Семюеля Морзе.

Спочатку азбуку Морзе застосовували для передавання повідомлень у телеграфі. При цьому крапки і тире передавалися у вигляді електричних сигналів, що проходять по дротах. Зараз азбуку Морзе, як правило, використовують у місцях, де інші засоби обміну інформацією недоступні (наприклад, у в'язницях).

Цікавий факт пов'язаний із винахідником першої лампочки Томасом Альвою Едісоном (1847-1931 рр.). Він погано чув і спілкувався зі своєю дружиною, Мері Стіуелл, за допомогою азбуки Морзе. Під час залицяння Едісон освідчився, відстукавши слова рукою, і вона відповіла у той самий спосіб. Телеграфний код став звичайним засобом спілкування для подружжя. Навіть коли вони ходили в театр, Едісон клав руку Мері собі на коліно, щоб вона могла "телеграфувати" йому діалоги акторів.

ТАБЛИЦЯ КОДУВАННЯ АЗБУКИ МОРЗЕ ТА ПРИКЛАД КОДУВАННЯ

Закодоване повідомлення	Таблиця кодування	Декодоване повідомлення
— • • — — — — • • • • — • — • — — • — — — — • • • — • — • • —	А •– Б –••• В •–– Г ––• Ґ ––• Д –•• Е • Є ••–•• Ж •••– З ––•• И ••– І •• Ї •––•– Й •––– К –•– Л •–•• М –– Н –• О ––– П •––• Р •–• С ••• Т – У ••– Ф ••–• Х –––– Ц –•–• Ч –––• Ш –––– Щ ––•–– Ь –••– Ю ••–– Я •–•– 1 •–––– 2 ••––– 3 •••–– 4 ••••– 5 ••••• 6 –•••• 7 ––••• 8 –––•• 9 ––––• 0 –––––	ДОБРИЙ ДЕНЬ

КОД БОДО

Код Бодо – цифровий 5-бітний код. Був розроблений Емілем Бодо в 1870 р. для свого телеграфа. Код вводили прямо клавіатурою, що складалася з п'яти клавіш, натискання або ненатискання клавіші відповідало передаванню або непередаванню одного біта в п'ятибітному коді. Існує кілька різновидів (стандартів) цього коду (CCITT-1, CCITT-2, МТК-2 та ін.) Зокрема, МТК-2 є модифікацією міжнародного стандарту CCITT-2 з додаванням букв кирилиці.

Співробітники телеграфної компанії AT&T Гільберто Вернам і Мейджор Джозеф Моборн у 1917 р. запропонували ідею автоматичного шифрування телеграфних повідомлень на основі коду Бодо. Шифрування виконувалося методом гамування по модулю 2.

КОД БОДО

(No Model.) 11 Sheets—Sheet 6.

J. M. E. BAUDOT.

PRINTING TELEGRAPH.

No. 388,244. Patented Aug. 21, 1888.

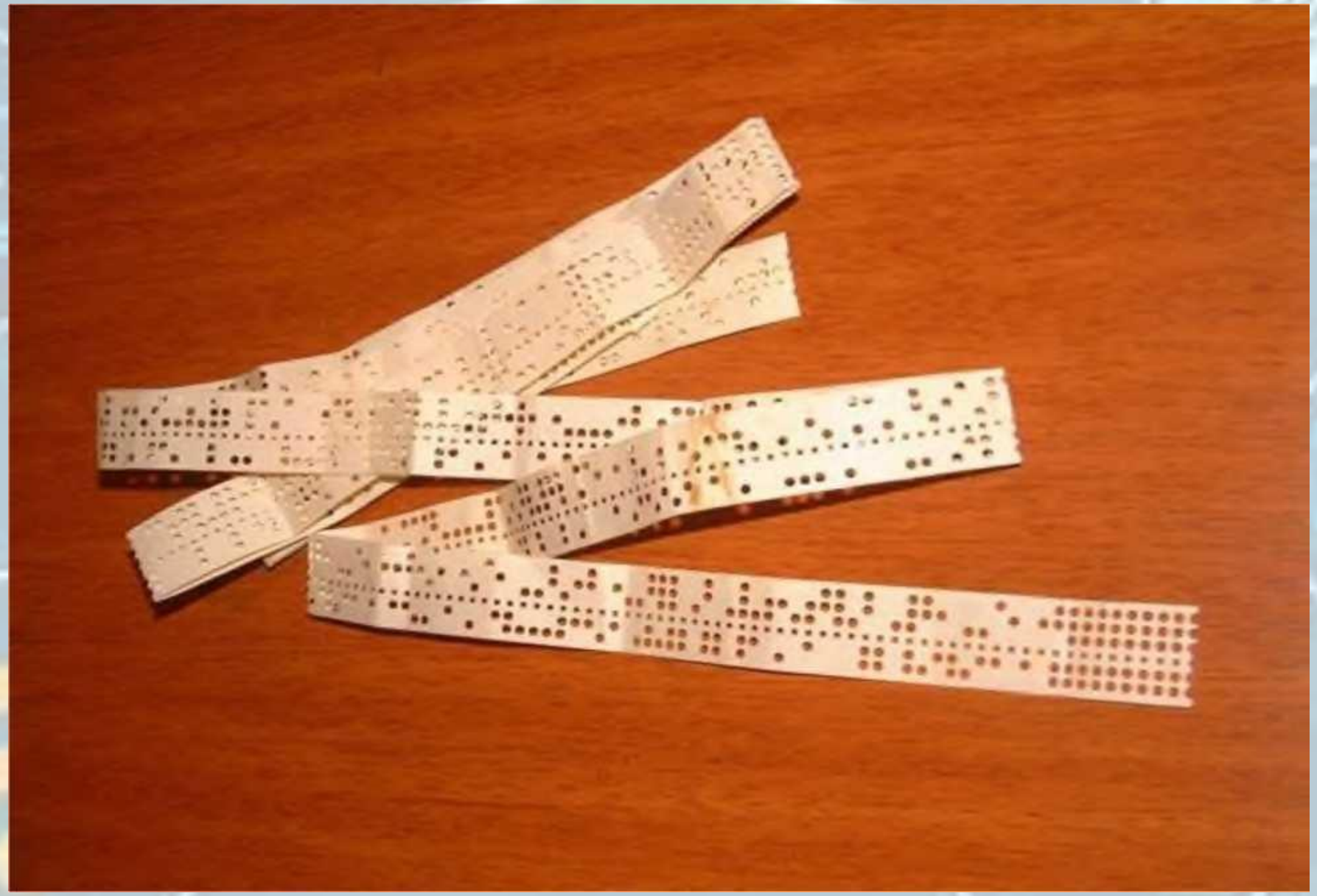
Fig. 24.

	1	2	3	4	5
A	+	−	−	−	−
B	−	−	+	+	−
C	+	−	+	+	−
D	+	+	−	−	−
E	−	+	−	+	−
F	−	+	+	+	−
G	+	+	+	−	−
H	+	−	−	+	−
I	−	+	−	+	−
J	+	+	−	+	−
K	+	+	+	+	+
L	−	+	+	+	+
M	+	+	+	−	+
N	−	+	+	+	+
O	+	+	+	+	−
P	+	+	+	−	+
Q	+	−	+	+	+
R	−	−	+	−	+
S	+	−	+	−	+
T	−	−	+	−	+
U	+	+	+	−	−
V	+	+	−	−	−
W	−	−	+	−	−
X	+	−	−	−	+
Y	−	−	−	+	+
Z	+	−	−	+	−
↕	−	−	−	−	+

INVENTOR:

Jean Maurice Emile Baudot

ПЕРФОСТРІЧКА З КОДОМ БОДО



ASCII I UNICODE

ASCII (англ. American Standard Code for Information Interchange) – американська стандартна кодувальна таблиця для друкованих і керуючих символів. Спочатку була розроблена як 7-бітна для представлення 128 символів. Під час використання в комп'ютерах на символ виділялося 8 біт (1 байт), де 8-ий біт часто слугував для контролю цілісності (парний паритетний біт). Пізніше, із задіянням 8 біта для представлення додаткових символів (всього 256 символів), наприклад букв національних алфавітів, стала сприйматися як половина 8-бітної. Зокрема, на основі ASCII було розроблено кодування, що містять літери українського алфавіту: для операційної системи MS-DOS – cp866 (англ. code page - кодова сторінка), для операційної системи MS Windows – Windows 1251, ISO 8859-5 та інші.

ТАБЛИЦЯ СИМВОЛІВ ASCII

символ	10-й код	2-й код	символ	10-й код	2-й код	символ	10-й код	2-й код	символ	10-й код	2-й код
	32	00100000	8	56	00111000	P	80	01010000	h	104	01101000
!	33	00100001	9	57	00111001	Q	81	01010001	i	105	01101001
"	34	00100010	:	58	00111010	R	82	01010010	j	106	01101010
#	35	00100011	;	59	00111011	S	83	01010011	k	107	01101011
$	36	00100100	<	60	00111100	T	84	01010100	l	108	01101100
%	37	00100101	=	61	00111101	U	85	01010101	m	109	01101101
&	38	00100110	>	62	00111110	V	86	01010110	n	110	01101110
'	39	00100111	?	63	00111111	W	87	01010111	o	111	01101111
(	40	00101000	@	64	01000000	X	88	01011000	p	112	01110000
)	41	00101001	A	65	01000001	Y	89	01011001	q	113	01110001
*	42	00101010	B	66	01000010	Z	90	01011010	r	114	01110010
+	43	00101011	C	67	01000011	[	91	01011011	s	115	01110011
,	44	00101100	D	68	01000100	\	92	01011100	t	116	01110100
-	45	00101101	E	69	01000101	]	93	01011101	u	117	01110101
.	46	00101110	F	70	01000110	^	94	01011110	v	118	01110110
/	47	00101111	G	71	01000111	_	95	01011111	w	119	01110111
0	48	00110000	H	72	01001000	`	96	01100000	x	120	01111000
1	49	00110001	I	73	01001001	a	97	01100001	y	121	01111001
2	50	00110010	J	74	01001010	b	98	01100010	z	122	01111010
3	51	00110011	K	75	01001011	c	99	01100011	{	123	01111011
4	52	00110100	L	76	01001100	d	100	01100100	|	124	01111100
5	53	00110101	M	77	01001101	e	101	01100101	}	125	01111101
6	54	00110110	N	78	01001110	f	102	01100110	~	126	01111110
7	55	00110111	O	79	01001111	g	103	01100111	□	127	01111111

ТАБЛИЦЯ КОДУВАННЯ WINDOWS 1251

128	Ъ	144	ђ	160		176	°	192	А	208	Р	224	а	240	р
129	Ѓ	145	‘	161	Ў	177	±	193	Б	209	С	225	б	241	с
130	‚	146	’	162	ў	178	І	194	В	210	Т	226	в	242	т
131	ѓ	147	“	163	Ј	179	і	195	Г	211	У	227	г	243	у
132	„	148	”	164	¤	180	ґ	196	Д	212	Ф	228	д	244	ф
133	…	149	•	165	Ґ	181	µ	197	Е	213	Х	229	е	245	х
134	†	150	–	166	¦	182	¶	198	Ж	214	Ц	230	ж	246	ц
135	‡	151	—	167	§	183	·	199	З	215	Ч	231	з	247	ч
136	’	152		168	Ё	184	ё	200	И	216	Ш	232	и	248	ш
137	‰	153	™	169	©	185	№	201	Й	217	Щ	233	й	249	щ
138	Љ	154	љ	170	Є	186	є	202	К	218	Ъ	234	к	250	ъ
139	‹	155	›	171	«	187	»	203	Л	219	Ы	235	л	251	ы
140	Њ	156	њ	172	¬	188	ј	204	М	220	Ь	236	м	252	ь
141	Ќ	157	ќ	173	-	189	S	205	Н	221	Э	237	н	253	э
142	Ћ	158	ћ	174	®	190	s	206	О	222	Ю	238	о	254	ю
143	Џ	159	џ	175	Ї	191	ї	207	П	223	Я	239	п	255	я

ASCII I UNICODE

Unicode – стандарт кодування символів, що дає змогу представити знаки майже всіх письмових мов. Стандарт був запропонований у 1991 р. некомерційною організацією "Консорціум Юнікоду" (англ. Unicode Consortium, Unicode Inc.). Застосування цього стандарту дає змогу закодувати більшу кількість символів (ніж в ASCII та інших кодуваннях) за рахунок двобайтового кодування символів (усього 65536 символів). У документах Unicode можуть бути сусідами китайські ієрогліфи, математичні символи, літери грецького алфавіту, латиниці та кирилиці.

Коди в стандарті Unicode розділені на кілька розділів. Перші 128 кодів відповідають кодуванню ASCII. Далі розташовані розділи літер різних писемностей, знаки пунктуації та технічні символи.

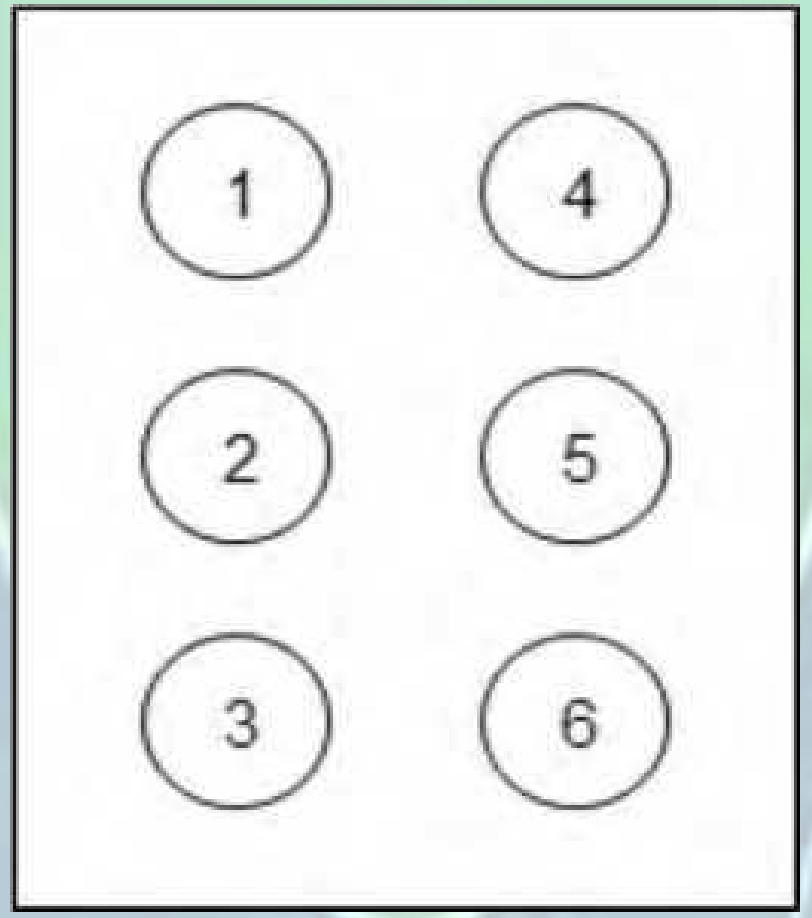
ШРИФТ БРАЙЛЯ

Шрифт Брайля – рельєфно-крапковий тактильний шрифт, призначений для письма і читання незрячими людьми. Був розроблений у 1824 р. французом Луї Брайлем (Louis Braille), сином шевця. Луї у віці трьох років втратив зір унаслідок запалення очей, що почалося від того, що хлопчик поранився шорним ножем (подібність шила) у майстерні батька. У віці 15 років він створив свій рельєфно-крапковий шрифт, надихнувшись простотою "нічного шрифту" капітана артилерії Шарля Барб'є (Charles Barbier), який використовували військові того часу для читання донесень у темряві.

Для зображення символів (здебільшого літер і цифр) у шрифті Брайля використовують 6 точок, розташованих у два стовпчики, по 3 у кожному.

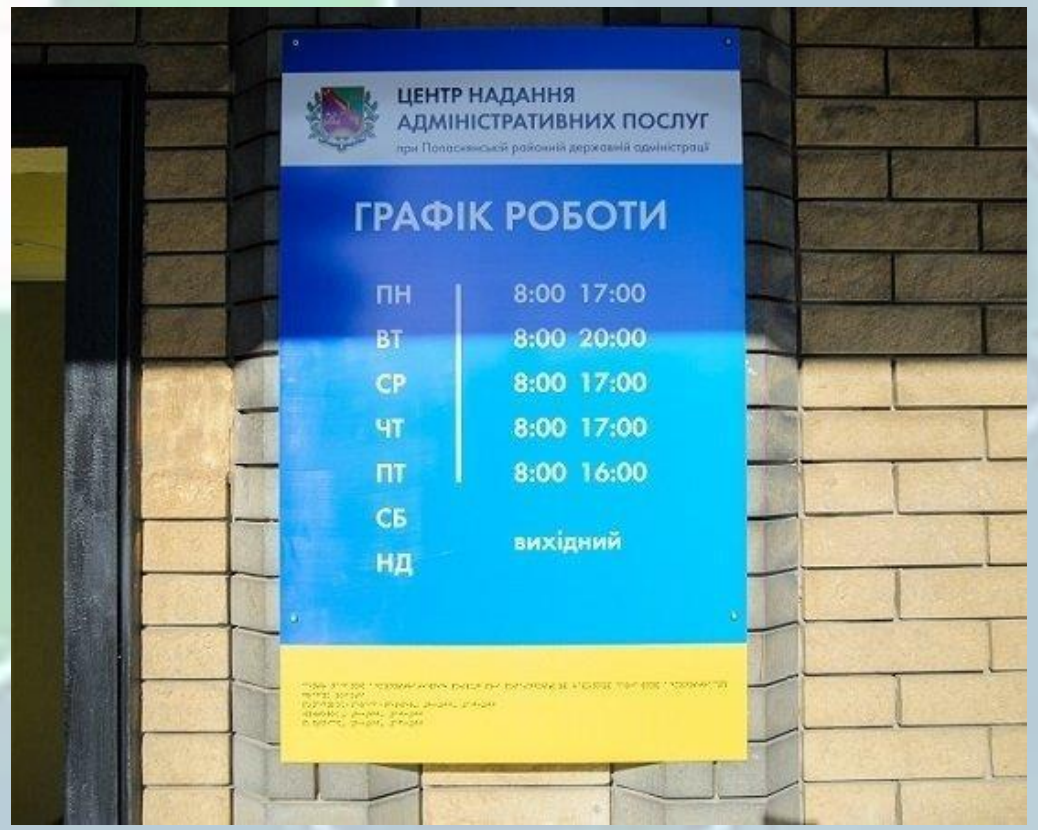
Кожному символу відповідає свій унікальний набір опуклих точок. Таким чином, шрифт Брайля являє собою систему для кодування $2^6 = 64$ символів. Але присутність у шрифті керівних символів (наприклад, перехід до букв або цифр) дає змогу збільшити кількість кодованих символів.

НУМЕРАЦІЯ ТОЧОК В ШРИФТІ БРАЙЛЯ



ШРИФТ БРАЙЛЯ

ПРИКЛАДИ ВИКОРИСТАННЯ ШРИФТУ БРАЙЛЯ



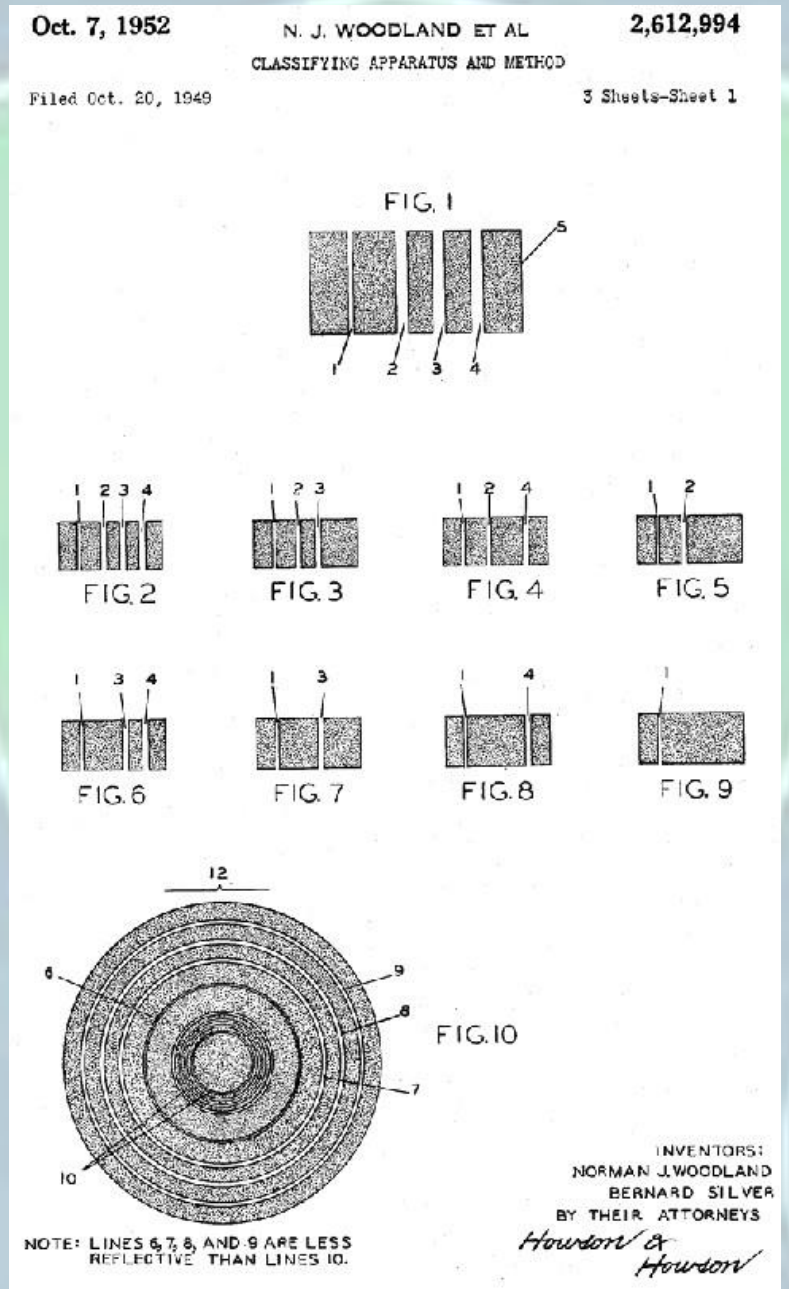
ШТРИХКОД

Штрихкод – графічна інформація, що наноситься на поверхню, маркування або упаковку виробів і являє собою послідовність чорних і білих смуг або інших геометричних фігур з метою її зчитування технічними засобами.

У 1948 р. Бернард Сільвер (Bernard Silver), аспірант Інституту Технології Університету Дрекселя у Філадельфії, почув, як президент місцевої продовольчої мережі просив одного з деканів розробити систему, що автоматично зчитує інформацію про продукт під час його контролю. Сільвер розповів про це друзям - Норману Джозефу Вудланду (Norman Joseph Woodland) і Джордіну Джохенсону (Jordin Johanson). Утрьох вони почали досліджувати різні системи маркування. Їхня перша працююча система використовувала ультрафіолетове чорнило, але воно було досить дорогим, а крім того, з часом вицвітало.

Переконаний у тому, що систему можна реалізувати, Вудланд покинув Філадельфію і перебрався до Флориди у квартиру свого батька для продовження роботи. 20 жовтня 1949 р. Вудланд і Сільвер подали заявку на винахід, яку було задоволено 7 жовтня 1952 р. Замість звичних нам ліній патент містив опис штрихкодової системи у вигляді концентричних кіл.

ПАТЕНТ СИСТЕМИ ВУДЛАНДА І СІЛЬВЕРА З КОНЦЕНТРИЧНИМИ КОЛАМИ, ПОПЕРЕДНИКАМИ СУЧАСНИХ ШТРИХКОДІВ



Oct. 7, 1952 N. J. WOODLAND ET AL 2,612,994

CLASSIFYING APPARATUS AND METHOD

Filed Oct. 20, 1949 3 Sheets-Sheet 1

FIG. 1

FIG. 2

FIG. 3

FIG. 4

FIG. 5

FIG. 6

FIG. 7

FIG. 8

FIG. 9

FIG. 10

NOTE: LINES 6, 7, 8, AND 9 ARE LESS REFLECTIVE THAN LINES 10.

INVENTORS:
NORMAN J. WOODLAND
BERNARD SILVER
BY THEIR ATTORNEYS
Howson & Howson

ШТРИХ-КОД

Уперше штрихкоди почали офіційно використовувати в 1974 р. у магазинах м. Трой, штат Огайо. Системи штрихового кодування знайшли широке застосування в суспільному житті: торгівля, поштові відправлення, фінансові та судові повідомлення, облік одиниць зберігання, ідентифікація осіб, контактна інформація (веб-посилання, адреси електронної пошти, телефонні номери) тощо.

Розрізняють **лінійні** (що читаються в одному напрямку) і **двовимірні штрихкоди**. Кожен із різновидів різниться як розмірами графічного зображення, так і обсягами поданої інформації. У наступній таблиці наведено приклади деяких різновидів штрихкоду.

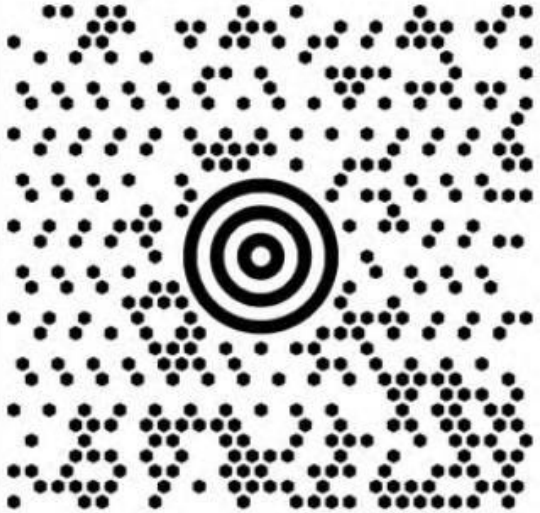
РІЗНОВИДИ ШТРИХКОДІВ

Найменування	Приклад штрих-коду	Примітки
	Лінійні	
Universal Product Code, UPC (універсальний код товару)	 (UPC-A)	Американський стандарт штрихкоду, призначений для кодування ідентифікатора товару і виробника. Є різновиди: - UPC-E - кодуються 8 цифр; - UPC-A - кодується 13 цифр.
European Article Number, EAN (європейський номер товару)	 (EAN-13)	Європейський стандарт штрихкоду, призначений для кодування ідентифікатора товару і виробника. Є різновиди: - EAN-8 - кодуються 8 цифр; - EAN 13 - кодується 13 цифр; - EAN-128 - кодується будь-яка кількість літер і цифр, об'єднаних у регламентовані групи. ГОСТ ІСО/МЕК 15420-2001 "Автоматична ідентифікація. Кодування штрихове. Специфікація символіки EAN/UPC (ЕАН/ЮПіСі)".

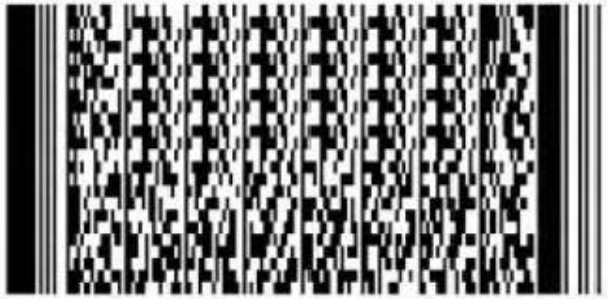
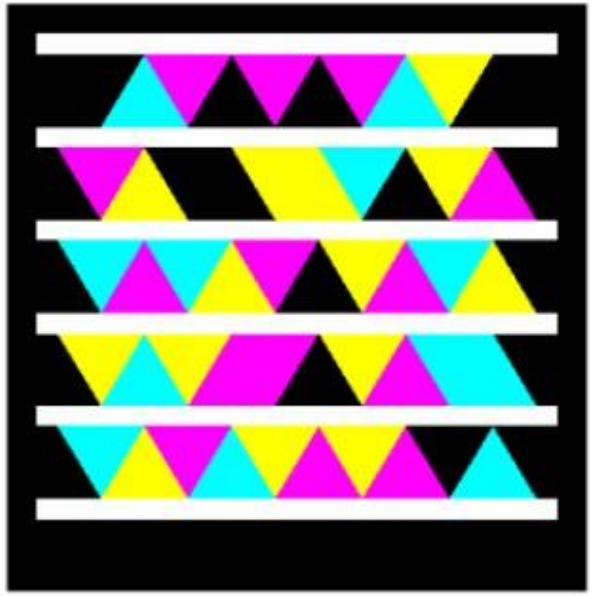
РІЗНОВИДИ ШТРИХКОДІВ

Найменування	Приклад штрих-коду	Примітки
Code 128 (Код 128)		Містить 107 символів, з яких 103 символи даних, 3 стартових, і 1 зупинний символ. Для кодування всіх 128-ми символів ASCII передбачено три комплекти символів - A, B і C, які можуть використовуватися всередині одного штрихкоду. EAN-128 кодує інформацію за алфавітом Code 128. ГОСТ 30743-2001 (ІСО/МЕК 15417-2000) "Автоматична ідентифікація. Кодування штрихове. Специфікація символіки Code 128 (Код 128)".
	Двовимірні	
DataMatrix (матричні дані)		Максимальна кількість символів, що поміщаються в один код - 2048 байт. ГОСТ Р ІСО/МЕК 16022-2008 "Автоматична ідентифікація. Кодування штрихове. Специфікація символіки Data Matrix".

РІЗНОВИДИ ШТРИХКОДІВ

Найменування	Приклад штрих-коду	Примітки
QR-код (англ. quick response - швидкий відгук)		Квадрати в кутах зображення дають змогу нормалізувати розмір зображення та його орієнтацію, а також кут, під яким сенсор відноситься до поверхні зображення. Точки переводяться в двійкові числа з перевіркою контрольної суми. Максимальна кількість символів, що вміщуються в один QR-код: - цифри - 7089; - цифри і букви (латиниця) - 4296; - двійковий код - 2953 байт; - ієрогліфи - 1817.
MaxiCode (максикод)		Розмір - дюйм на дюйм (1 дюйм = 2.54 см). Використовується для вантажовідправних і вантажоприймальних систем. Може вмістити в себе стільки ж символів, що Code128. ГОСТ Р 51294.6-2000 "Автоматична ідентифікація. Кодування штрихове. Специфікація символіки MaxiCode (Максикод)".

РІЗНОВИДИ ШТРИХКОДІВ

Найменування	Приклад штрих-коду	Примітки
PDF147 (англ. Portable Data File - портативний файл даних. переносимий файл даних)		Застосовується під час ідентифікації особи, обліку товарів, під час здавання звітності до контролюючих органів та в інших сферах. Підтримує кодування до 2710 символів і може містити до 90 рядків.
Microsoft Tag (мітка Microsoft)		Розроблено для розпізнавання за допомогою фотокамер, вбудованих у мобільні телефони. Може вмістити в себе стільки ж символів, що Code128. Призначений для швидкої ідентифікації та отримання на пристрій заздалегідь підготовленої інформації (веб-посилання, довільного тексту довжиною до 1000 символів, телефонного номера тощо), прив'язаної до коду, яка зберігається на сервері компанії Microsoft. Містить 13 байт плюс один додатковий біт для контролю парності.

ПРЕДСТАВЛЕННЯ ЧИСЕЛ У ДВІЙКОВОМУ ВИГЛЯДІ (У КОМП'ЮТЕРІ)

Як відомо, інформація, що зберігається й обробляється в комп'ютерах, представлена в двійковому вигляді. ***Біт*** (англ. binary digit – двійкове число; також гра слів: англ. bit – шматочок, частинка) – одиниця виміру кількості інформації, що дорівнює одному розряду в двійковій системі числення. За допомогою біта можна закодувати (уявити, розрізняти) два стани (0 або 1; так чи ні). Збільшуючи кількість бітів (розрядів), можна збільшити кількість кодованих станів. Наприклад, для байта (англ. byte), що складається з 8 бітів, кількість кодованих станів становить $2^8 = 256$.

Числа кодуються в так званих форматах із фіксованою та плаваючою комою.

ГЕНЕТИЧНИЙ КОД

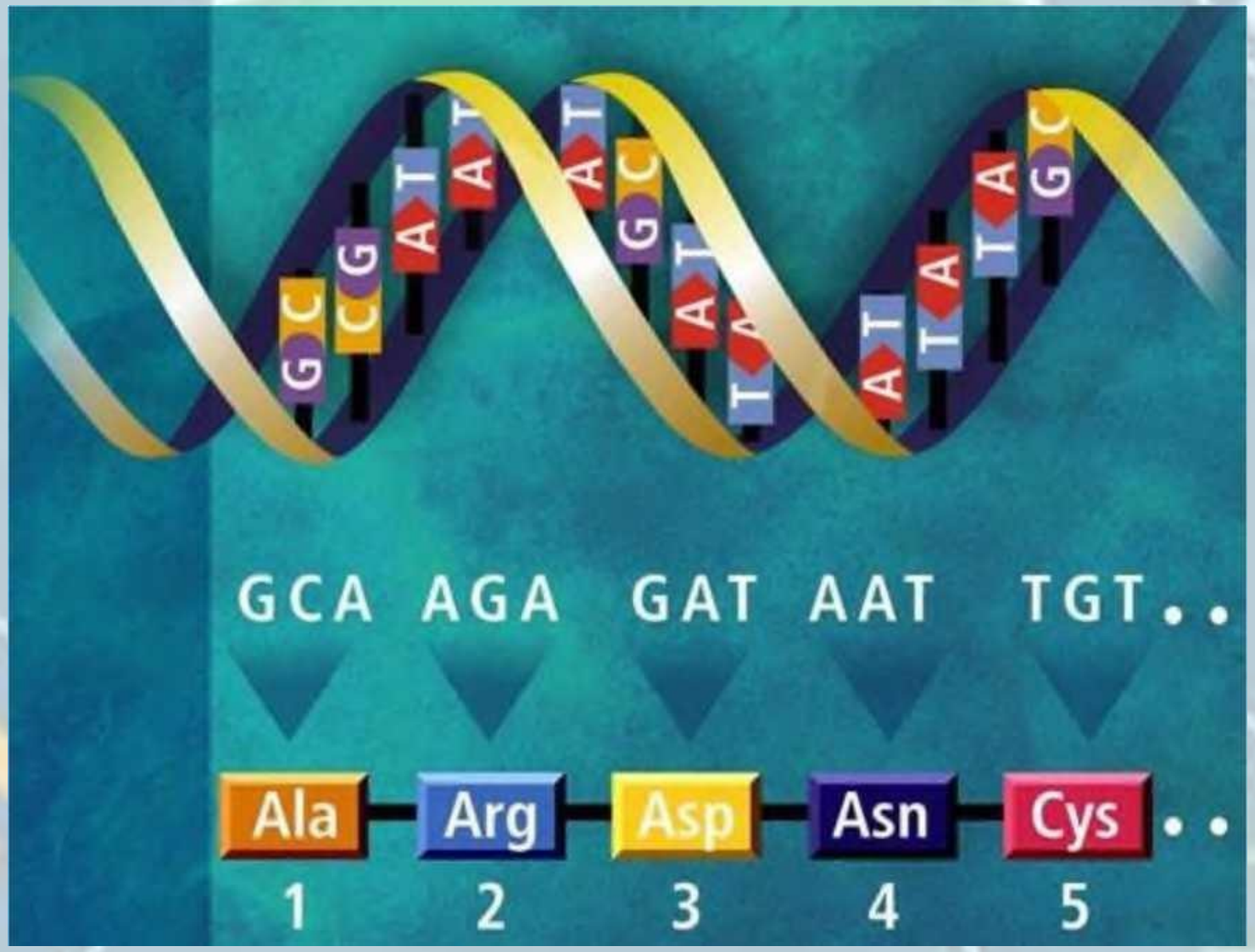
Генетичний код – властива всім живим організмам кодована амінокислотна послідовність білків. Кодування виконується за допомогою нуклеотидів, що входять до складу ДНК (дезоксирибонуклеїнової кислоти). **ДКН** – макромолекула, що забезпечує зберігання, передачу з покоління в покоління і реалізацію генетичної програми розвитку та функціонування живих організмів. Мабуть, найголовніший код в історії людства.

ГЕНЕТИЧНИЙ КОД

У ДНК використовується чотири азотисті основи – аденін (A), гуанін (G), цитозин (C), тимін (T), які в україномовній літературі позначають буквами А, Г, Ц і Т. Ці літери складають алфавіт генетичного коду. У молекулах ДНК нуклеотиди шикуються в ланцюжки і, таким чином, виходять послідовності генетичних букв.

Білки практично всіх живих організмів побудовані з амінокислот усього 20 видів. Ці амінокислоти називають канонічними. Кожен білок являє собою ланцюжок або кілька ланцюжків амінокислот, з'єднаних у суворо визначеній послідовності. Ця послідовність визначає будову білка, а отже, всі його біологічні властивості. Синтез білків (тобто реалізація генетичної інформації в живих клітинах) здійснюється на основі інформації, закладеної в ДНК. Для кодування кожної з 20 амінокислот, а також сигналу "стоп", що означає кінець білкової послідовності, достатньо трьох послідовних нуклеотидів (триплету).

ФРАГМЕНТ ДНК



ПИТАННЯ №5

СЕКРЕТНІ КОДОВІ СИСТЕМИ

СЕКРЕТНІ КОДОВІ СИСТЕМИ

Секретні коди, як і шифри, призначені для забезпечення конфіденційності інформації. Спочатку секретні кодові системи являли собою стеганографічну систему, в основі якої лежала подоба жаргонного коду. Вони виникли з метою приховування імен реальних людей, які згадувалися в листуванні. Це були невеликі списки, в яких було записано приховувані імена, а навпроти них - кодові заміни (підстановки). Офіційні коди для приховування змісту донесень, якими користувалися папські емісари та посли середземноморських міст-держав, знайдені в ранніх архівах Ватикану, датуються XIV ст. У міру зростання потреби в безпеці листування у представників міст-держав з'явилися ширші переліки, що містили в собі не тільки кодові заміни імен людей, а й країн, міст, видів зброї, провіанту і т. д. З метою підвищення захищеності інформації до переліків додали шифралфавіти для кодування слів, що не увійшли до переліку, а також правила їх використання, що базуються на різних стеганографічних і криптографічних методах. Такі збірники отримали назву **"номенклатори"**. З XV і до середини XIX ст. вони були основною формою забезпечення конфіденційності інформації.

СЕКРЕТНІ КОДОВІ СИСТЕМИ

Аж до XVII століття в номенклаторах слова відкритого тексту та їхні кодові заміни йшли в алфавітному порядку, поки французький криптолог Антуан Россіньйоль не запропонував використовувати більш стійкі номенклатори, які складалися з двох частин. У них існувало два розділи: в одному перераховувалися в алфавітному порядку елементи відкритого тексту, а кодові елементи були перемішані. У другій частині в алфавітному порядку йшли переліки кодів, а перемішаними були вже елементи відкритого тексту.

Винахід телеграфу й азбуки Морзе, а також прокладання трансатлантичного кабелю в середині XIX ст. значно розширило сфери застосування секретних кодів. Крім традиційних сфер їхнього використання (у дипломатичному листуванні та у військових цілях) вони стали широко використовуватися в комерції і на транспорті. Секретні кодові системи того часу у своїй назві містили слово **"код"** ("Код Держдепартаменту (1867 р.)", "Американський код для окопів", "Річкові коди: Потомак", "Чорний код") або **"шифр"** ("Шифр Держдепартаменту (1876 р.)", "Зелений шифр"). Слід зазначити, що, незважаючи на наявність у назві слова "шифр", в основу цих систем було покладено кодування.

Розробники кодів, як і укладачі шифрів, нерідко додавали додаткові ступені захисту, щоб ускладнити злом своїх кодів. Такий процес називається перешифруванням. У підсумку секретні кодові системи поєднували в собі як стеганографічні, так і криптографічні способи забезпечення конфіденційності інформації.

СПОСОБИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В СЕКРЕТНИХ КОДОВИХ СИСТЕМАХ

Спосіб	Тип	Примітки	Приклади (кодоване слово - кодове позначення)
Заміна слова (словосполучення) іншим словом довільної довжини	стеганографічний	Аналог - жаргонний код. Для одного кодованого слова могли використовуватися кілька кодових позначень.	1. Номенклатор міста Сієни (XV ст.): Cardinales (кардинал) - Florenus; Antonello da Furli (Антолло да Фурлі) - Forte. 2. Шифр Держдепартаменту 1899 р.: Russia (Росія) - Promotes; Cabinet of Russia (Уряд Росії) - Promptings. 3. Код керівника служби зв'язку (1871 р.): 10:30 - Anna, Ida; 13th (тринадцятий) - Charles, Mason.
Заміна слова (словосполучення) символьним рядком фіксованої довжини	стеганографічний	Аналог - жаргонний код.	1 Американський код для окопів (1918 р.): Patrol (патруль) - RAL; Attack (атака) - DIT. 2. Код Держдепартаменту А-1 (1919 р.): Diplomat (дипломат) - BUJOH; Diplomatic corps (дипломатичний корпус) - BEDAC.

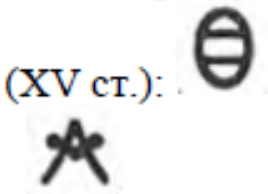
СПОСОБИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В СЕКРЕТНИХ КОДОВИХ СИСТЕМАХ

Спосіб	Тип	Примітки	Приклади (кодоване слово - кодове позначення)
Заміна слова (словосполучення) числом	стеганографічний	Аналог - жаргонний код. Для одного кодованого слова могли використовуватися кілька кодових позначень.	1. Номенклатор Бенджаміна Толмаджа (1779 р.): Defense (оборона) - 143; Attack (атака) - 38. 2. Код мовлення для торгових суден союзників у Другій світовій війні (BAMS): острів - 36979; порт - 985.
Заміна слова (словосполучення) набором цифр фіксованої довжини	стеганографічний	Аналог - жаргонний код.	1 Американський код для окопів (1918 р.): Patrol (патруль) - 2307; Attack (атака) - 1447. 2. Американський службовий радіокод № 1 (1918 р.): Oil (масло) - 001; Bad (поганий) - 642.

СПОСОБИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В СЕКРЕТНИХ КОДОВИХ СИСТЕМАХ

Спосіб	Тип	Примітки	Приклади (кодоване слово - кодове позначення)
Заміна букв	криптографічний	Аналоги - шифр однозначної заміни, омофонічний шифр, поліалфавітний шифр. Як кодове позначення могли використовуватися букви, числа, графічні позначення. Застосовувалася для слів, відсутніх у списку кодованих.	1. Номенклатор міста Сієни (XV ст.): q -  ; s -  . 2. Номенклатор Джеймса Медісона (1781 р.): o - 527; p - 941. 3. Американський код для окопів (1918 р.): a - 1332 ... 2795 або CEW ... ZYR. Містив також 30 алфавітів шифрозамін для перешифрування кодових позначень.
Заміна поєднання букв	криптографічний	Аналог - поліграмний шифр заміни. Як кодове позначення могли використовуватися букви, числа, графічні позначення.	1. Номенклатор міста Сієни (XV ст.): bb -  ; tt -  . 2. Номенклатор X-Y-Z (1737 р.): ce - 493; ab - 1194.

СПОСОБИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В СЕКРЕТНИХ КОДОВИХ СИСТЕМАХ

Спосіб	Тип	Примітки	Приклади (кодоване слово - кодове позначення)
Використання порожніх знаків	стеганографічний	Аналог - пустушковий шифр. Символи, що нічого не призначали (лат. nihil importantes), використовували для заплутування криптоаналітиків.	1. Номенклатор міста Сієни (XV ст.):  . 2. Річкові коди: Потомак (1918 р.): ASY.
Використання адитивних чисел	криптографічний	Аналог - поліалфавітний шифр. Адитивне число, що додається до числового кодового позначення, слугувало змінною частиною коду (ключа).	Шифр Держдепартаменту 1876 р.: правило "Horse" (кінь) на початку повідомлення означало, що під час кодування наступних кодових позначень використовували адитивне число 203; "Hawk" (яструб) - 100.

СПОСОБИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В СЕКРЕТНИХ КОДОВИХ СИСТЕМАХ

Спосіб	Тип	Примітки	Приклади (кодоване слово - кодове позначення)
Перестановка букв (цифр) у кодових позначеннях	криптографічний	Аналог - шифр блокової одинарної перестановки.	Телеграфний код для забезпечення секретності під час передавання телеграм (1870 р.): одне з правил наказувало перестановку останніх трьох цифр у цифровому кодовому позначенні, яке складається з п'яти цифр.
Перестановка кодових позначень	криптографічний	Аналог - шифр перестановки.	Шифр Держдепартаменту 1876 р.: правило "Tiger" (тигр) на початку повідомлення означало, що розкодоване повідомлення треба читати з останнього слова по перше (задом наперед); "Tapir" (тапір) - міняючи місцями кожну пару слів (тобто перше та друге, третє та четверте і т.д.).

ЧЕРВОНА І СИНЯ КНИГИ

Поєднання різних способів кодування і перешифровки в кодовій системі було звичайною практикою у розробників кодів і стало застосовуватися практично від самого початку їхньої появи. Так, ще в номенклаторі, який використовували в м. Сієна в XV ст., крім кодових замін слів, застосовували шифралфавіти для заміни букв, їх подвоєних поєднань і порожніх знаків. Найбільшого розквіту ця практика набула наприкінці XIX – початку XX ст. **Зокрема, у "Шифрі Держдепартаменту 1876 р." (англ. Red Book – Червона книга), що складався з 1200 сторінок, і його доповненні "Код, що не піддається декодуванню: доповнення до шифру Держдепартаменту" застосовувалися:**

- кодові позначення у вигляді слів і чисел;
- 30 шифралфавітів для заміни букв;
- 50 правил перешифрування, включно з адитивними числами, перестановками кодових позначень та їхніх частин.

У **доповненні до "Шифру Держдепартаменту 1899 р." (англ. Blue Book – Синя книга)** було описано ще 25 додаткових правил перешифрування: зміна напряму читання і запису, додавання або віднімання чисел, заміна кодових чисел іншими кодовими числами.

КНИЖКОВІ КОДИ

Розробники кодів, щоб закодувати повідомлення, можуть не тільки створювати від самого початку нові коди, а й скористатися вже наявними текстами. Так звані **книжкові коди** за своєю суттю аналогічні книжковому шифру. На відміну від них заміні підлягає не буква, а все слово цілком. Таким чином, кодова заміна являє собою трійку чисел "сторінка.рядок.слово". У книжкових шифрах, як і в кодових системах, розглянутих вище, знайшли широке застосування різні способи перешифрування. Зокрема, адитивні числа, перестановки цифр і повторні заміни.

Безсумнівною перевагою книжкового коду є те, що виключається необхідність використовувати кодові книжки, що викликають підозру, – виявлення такої може призвести до провалу агента. Водночас саму книжку можна загубити або її можуть вкрасти, внаслідок чого виявиться скомпрометованою вся система.

ДЯКУЮ ЗА УВАГУ!