**ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № \_\_\_13\_\_\_\_\_**

**1. Система Діффі-Гелмана.**

Обмін ключами Діффі–Хеллмана встановлює спільний секрет між двома сторонами, який можна використовувати для секретного зв’язку для обміну даними через загальнодоступну мережу. Аналогія ілюструє концепцію обміну відкритими ключами за допомогою кольорів замість дуже великих чисел:

Процес починається з того, що дві сторони, Аліса та Боб , публічно погоджують довільний початковий колір, який не потрібно тримати в секреті. У цьому прикладі колір жовтий. Кожна людина також вибирає секретний колір, який залишає при собі – у цьому випадку червоний і блакитний. Вирішальною частиною процесу є те, що Аліса та Боб змішують кожен свій таємний колір зі своїм спільним кольором, у результаті чого утворюються помаранчево-коричневі та світло-блакитні суміші відповідно, а потім публічно обмінюються двома змішаними кольорами. Нарешті, кожен з них змішує колір, отриманий від партнера, зі своїм власним кольором. Результатом є кінцева суміш кольорів (у цьому випадку жовто-коричнева), яка ідентична кінцевій суміші кольорів їхнього партнера.

Якби третя сторона прослухала обмін, вона знала б лише загальний колір (жовтий) і перші змішані кольори (оранжево-коричневий і світло-блакитний), але їм було б дуже важко дізнатися остаточний секретний колір ( жовто-коричневий). Повернувши аналогію до обміну в реальному житті з використанням великих чисел, а не кольорів, це визначення є дорогим з точки зору обчислень. Навіть для сучасних суперкомп'ютерів неможливо виконати обчислення за практичний проміжок часу .

**2. Робота з камерами відеоспостережень. Пакети Netmeeting та Videoinspector.**

Про камери відеоспостереження:

Наразі використовуються два основні формати: аналоговий і цифровий.

Аналог передбачає безпосередню передачу зображення у вигляді електричного сигналу з матриці камери по кабелю до прийомного пристрою. Сигнал не проходить будь-яку обробку або шифровку. Аналоговий формат забезпечує мінімальну затримку в передачі картинки, однак, сильно піддається впливу перешкод і не захищає лінію від вторгнень.

Варто зазначити три «аналогових» формати: HD-TVI, HD-CVI і AHD. Аналог вказано в лапках, тому що спочатку використовувався аналоговий формат CVBS, який зараз зовсім втратив актуальність, а зазначені вище формати є його доопрацьованою версією. Камери формату HD-TVI, HD-CVI і AHD можуть використовувати старі аналогові лінії, при цьому передавати сигнал сучасного формату.

У цифровому варіанті сигнал передається у вигляді двійкового коду. Цей код фізично також є електричним сигналом, але з іншими властивостями. При використанні цифрового формату відео передається з невеликою затримкою, але при цьому зашифровано і може піддаватися додатковій обробці й аналітиці. Наприклад, можна стискати цифрове відео, чим зменшувати простір, який воно займає, при передачі і зберіганні. Також цифровий формат забезпечує більшу безпеку. Цифрові IP камери дозволяють вибирати пріоритетні ділянки для зйомки і можуть реагувати на поведінку об'єктів у кадрі

IP-відеоспостереження є найбільш сучасним. Основними причинами того, що аналоговий формат все ще використовується, є простіша установка і універсальність при виборі обладнання, а також його вартість, яка може відрізнятися в порівнянні з IP не на користь останнього.

Microsoft NetMeeting — застосунок для відеоконференцзв'язку, дозволяє організовувати аудіо- і відео-контакти (за наявності відеокамери) між двома і більше учасниками конференції.

Окрім цього, він має такі можливості:

* Пересилка файлів. У ході конференції Ви можете обмінюватися з користувачами файлами.
* Спільна робота над документом. Одна з найбільш відмітних особливостей NetMeeting — надає можливість сумісного використання застосунків. Наприклад, Ви можете дозволити працювати віддаленому співбесіднику з Вашими офісними програмами, причому, у видаленого користувача ці програми можуть бути не встановлені.
* Спілкування в чаті. Можливість обміну із співбесідником текстовими повідомленнями.
* «Біла» дошка (англ. whiteboard). Можливість обміну із співбесідником графічною інформацією в інтерактивному режимі. В цьому випадку у кожного учасника відкривається додаткове вікно зі всіма необхідними функціями. Всі Ваші дії (малювання, вставка фотографії, графіків тощо) тут же відображаються у партнера.

VideoInspector — безкоштовна утиліта , що працює під операційною системою Windows , що надає користувачам інструмент для перегляду детальної інформації про відео файли, а також його складових.

VideoInspector надає детальну інформацію про відео файл у системі, а також які кодеки потрібні (з наданням посилання для їх подальшого завантаження) для його відтворення і які вже є в наявності. Відповідно, програма може стати в нагоді у випадку, якщо в запущеному відео файлі відсутній звук, не відображається зображення або він не відтворюється .

До того ж, утиліта показує інформацію та інші атрибути файлу, наприклад, тривалість, інформацію про потоках , бітрейті , частоті каналу та інші.

Основні можливості утиліти:

* Контейнерна підтримка для форматів AVI , Matroska , MPEG-1 , MPEG-2 , QuickTime .
* Автоматичне виявлення кодеків , що вимагають .
* Список встановлених аудіо / відео кодеків .
* Редактор FourCC .
* Бітрейт .
* Аналіз пакетних файлів , а також експорт у CSV та HTML формати.
* Перевірка цілісності файлу.
* Завантаження необхідних кодеків (online база даних).
* Автоматичне виявлення вмісту контейнера.
* Відображення детальної інформації про фільм.
* Відображення інформації про відео / аудіо потоки.
* Обчислення якості відеофайлу.
* Запис CD / DVD (лише з CopyToDVD ).
* Інтеграція в Windows Shell ( Drag-and-drop та контекстне меню ).
* Міжнародна підтримка.

**3. Стеганографія. Пакет S-tools.**

Техніка стеганографії передбачає приховування конфіденційної інформації у звичайному, несекретному файлі чи повідомленні, щоб її не було виявлено. Потім конфіденційну інформацію буде витягнуто зі звичайного файлу або повідомлення в місці призначення, таким чином уникаючи виявлення. Стеганографія є додатковим кроком, який можна використовувати разом із шифруванням, щоб приховати або захистити дані.

Стеганографія — це засіб приховування секретної інформації в межах (або навіть поверх) звичайного, несекретного документа чи іншого носія, щоб уникнути виявлення. Воно походить від грецьких слів steganos, що означає «покритий» або «прихований», і graph, що означає «писати». Отже, «приховане письмо».

Ви можете використовувати стеганографію, щоб приховати текст, відео, зображення або навіть аудіодані. Це корисна частина знань, обмежена лише типом носія та уявою автора.

Різні типи стеганографії

1. Текстова стеганографія. У текстових файлах існує стеганографія, яка передбачає таємне зберігання інформації. У цьому методі приховані дані кодуються в літеру кожного слова.

2. Стеганографія зображення − Другим типом стеганографії є стеганографія зображення, яка передбачає приховування даних за допомогою зображення іншого об’єкта як прикриття. Інтенсивність пікселів є ключем до приховування даних у стеганографії зображень.

3. Аудіо стеганографія – це наука про приховування даних у звукі. У цифровому вигляді він захищає від несанкціонованого відтворення. Водяні знаки — це техніка, яка шифрує одну частину даних (повідомлення) в іншій («носій»). Його типове використання включає відтворення медіафайлів, насамперед аудіокліпів.

4. Стеганографія відео. Стеганографія відео – це метод таємного вбудовування даних або інших файлів у відеофайл на комп’ютері. Відео (набір нерухомих зображень) може функціонувати як «носій» у цій схемі. Дискретне косинусне перетворення (DCT) зазвичай використовується для вставки значень, які можна використовувати для приховування даних у кожному зображенні у відео, яке неможливо помітити неозброєним оком. Відеостеганографія зазвичай використовує такі формати файлів: H.264, MP4, MPEG і AVI.

5. Мережева або протокольна стеганографія – передбачає приховування даних за допомогою мережевого протоколу, як-от TCP, UDP, ICMP, IP тощо, як прикриття. Стеганографія може бути використана у випадку прихованих каналів, які виникають у моделі мережі рівня OSI.

Приклади стеганографії включають

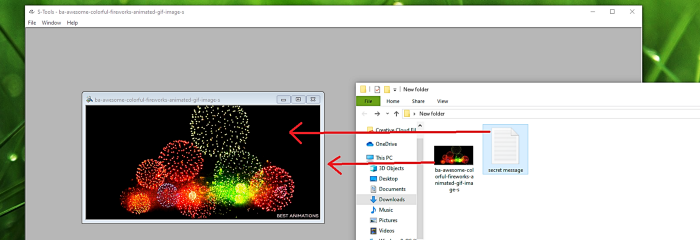
* Писати невидимим чорнилом
* Вбудовування тексту в малюнок (як художник ховає свої ініціали на картині, яку він написав)
* Зворотне маскування повідомлення в аудіофайлі (пам’ятаєте ті історії про злісні повідомлення, записані назад на рок-н-рольних платівках?)
* Приховування інформації в метаданих або в заголовку файлу
* Приховування зображення у відео, яке можна переглядати, лише якщо відео відтворюється з певною частотою кадрів
* Вбудовування секретного повідомлення в зелений, синій або червоний канал зображення RRB

Стеганографія — це метод, який дозволяє легко приховати повідомлення в іншому, щоб зберегти його в секреті. У результаті приховане повідомлення залишається прихованим. Стеганографічний підхід може принести користь зображенням, відео та аудіофайлам. Додаткові переваги включають:

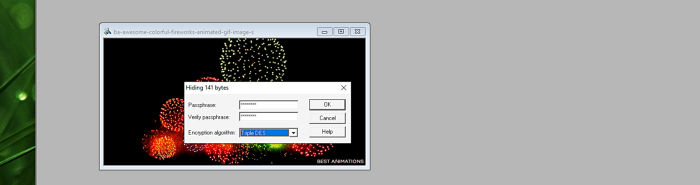
На відміну від інших методів, стеганографія має додаткову перевагу приховування комунікацій настільки добре, що вони не привертають уваги. Однак у країнах, де шифрування є незаконним, надсилання зашифрованого повідомлення, яке можна легко розшифрувати, викликає підозри та може бути ризикованим.

S-Tools — це програма, створена Енді Брауном. Можливо, це найпоширеніший інструмент стеганографії, доступний сьогодні. Ви можете використовувати типи файлів BMP, GIF і WAV для покриття документів, які приховують секретні дані. Простота інструменту дозволяє легко перетягувати файли. S-Tools приховає секретне повідомлення у файлі обкладинки за допомогою випадково доступних бітів. Ці доступні біти розрізняються за допомогою генератора псевдовипадкових чисел. Це нелінійне додавання робить присутність і вилучення секретних повідомлень все більш проблемним.

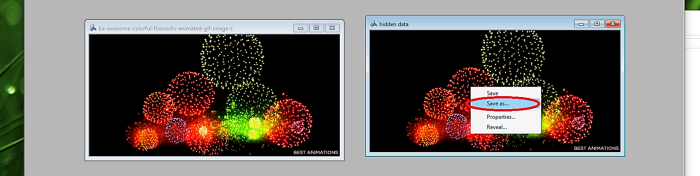
Як ми вже згадували раніше, користуватися цим інструментом дуже просто: перетягніть файл із зображенням обкладинки, а потім файл секретного повідомлення поверх нього.



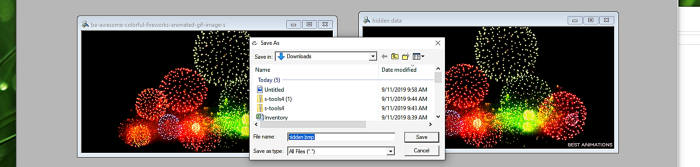
На головному дисплеї з’явиться невелике вікно з проханням зашифрувати файл stego. Створіть новий пароль для шифрування та натисніть кнопку «ОК» .



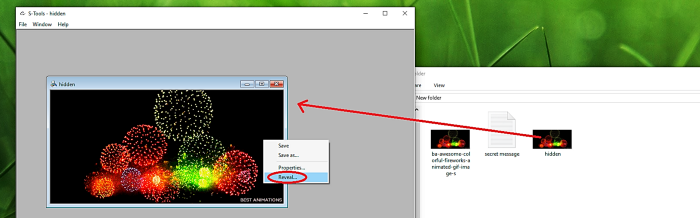
Це створить нове стего зображення. Щоб зберегти стего-файл, клацніть зображення правою кнопкою миші та виберіть опцію «Зберегти як…» .



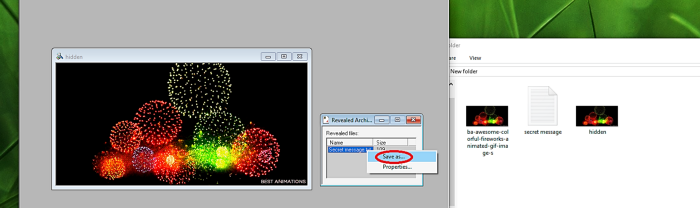
Вкажіть місце призначення для збереження стего-зображення та натисніть кнопку «Зберегти» .



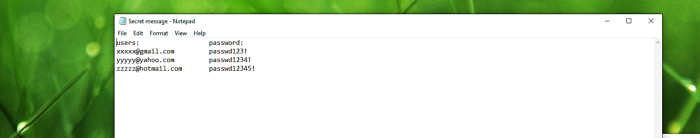
Щоб отримати приховану інформацію зі стего-зображення, запустіть S-Tools, а потім перетягніть туди файл. Клацніть правою кнопкою миші на зображенні та виберіть у спадному меню опцію «Відкрити…» .



Відкриється вікно «Розкритий архів» , у якому відображатиметься ім’я файлу секретного повідомлення. Клацніть правою кнопкою миші на імені файлу, а потім виберіть опцію «Зберегти як…» , щоб зберегти його у вибраному вами місці.



Після цього перейдіть до вказаного місця, і ви зможете переглянути файл секретного повідомлення.



S-Tools має розмір 589 Кб, і, як і багато інших програм стеганографії, не залишає жодних слідів. З іншого боку, S-Tools має добре відомий підпис. S-Tools зменшує кількість кольорів у файлі обкладинки до мінімуму 32. У результаті це впливає на зображення у відтінках сірого. Існує більш повний опис, але він виходить за рамки цієї статті. Підводячи підсумок, через зміни в індексах палітри справжнє зображення у відтінках сірого більше не може бути справжнім зображенням у відтінках сірого. Як результат, цей підпис палітри можна використовувати, щоб відрізнити одне зображення від іншого, яке містить прихований файл. З іншого боку, секретні дані мають дуже хороші шанси залишитися таємними завдяки надійному шифруванню, яке можна встановити.