1.Что такое стеганаграфия (СГ) и из каких двух основных частей она состоит?
СТЕГАНОГРАФИЯ - "Скрытие информации" (Information hiding (IH)).
IH - это семейство методов, при помощи которых некоторое дополнительное сведение погружается в основное (ПС) при сохранении хорошего качества ПС.
Две основные части IH:
1. Собственно стеганография (стеганография).
2. Цифровые "водяные знаки" (ЦВЗ).

2.Чем отличается СГ от криптографии ?
КР делает невозможным понимание содержание сообщения, сохраняя при этом возможность обнаружить факт ее использования (шумоподобные сигналы).
СГ утаивает сам факт погружения дополнительной информации в "невинное" сообщение.

3.Что означает применение принципа Керхгоффа к СГ?
Предполагается, что нелегитимным пользователям известно о IH-системе все, кроме стегоключа. Нелегитимный пользователь, который пытается нарушить выполнение задачи IH, называется атакующим (или злоумышленником), а его действия атакой на стегосистему.

4.Какие типы покрывающих сообщений используются в СГ ?
Типичные ПС:
- неподвижное изображение
- подвижное изображение (видео)
- аудио файлы
- речь
- печатный смысловой текст
- графические представления текста и схем
- интернет - протоколы
- программы для компьютеров.

Вкладываемая информация:
- изображение
- текстовые сообщения и данные
- речевые сообщения.

Как правило, все вкладываемые сообщения предварительно шифруются с использованием ключей шифрования.

5.Как определить такие понятия , как секретность СГ , искажение ПС , скорость передачи секретных сообщений и их достоверность?
Секретность СГ – невозможность обнаружения нелегитимными пользователями
Искажение ПС – ухудшение качества ПС (зернистость, полосы)
Скорость передачи СГ – зависит от пропускной способности передающего канала связи.
Достоверность СГ – устойчивое выделение скрытого сообщения при любых естественных или преднамеренных операциях, существенно не искажающих ПС.

6.Можно ли построить идеально необнаруживаемые СГ ?
СГС называется *идеальной* (*совершенной, безусловно необнаруживаемой*), если ее обнаружение, при использовании наилучших статистических методов, равносильно случайному угадыванию ее наличия или отсутствия.
1. Если ПС может выбираться и допустимо участие человека, то ИСГС реализуема в Л-СГС с использованием хеш-функций (х.ф.), (см. лекцию 4).
2. Если допустимо вложение даже малого количества бит, то ИСГС реализуема для любых выбираемых ПС автоматически с использованием х.ф. (такой метод называется еще *“rejection-sampling” – см. лекцию 4*).

3. Если в канале имеется естественный шум, то построение ИСГС, устойчивых к атаке удаления, возможно при малой скорости вложения (см. лекцию 6. “СГС в каналах с шумами”).
4. Если задана точная статистическая модель ПС, то построение ИСГС, устойчивой к атаке удаления, возможно (см. следующие разделы лекции).
5. Если статистическая модель ПС в точности не известна, то возможно построение ПИСГС с малой скоростью вложения (см.следующие разделы лекции).

7.Что означает вложение в наименьшие значащие биты (НЗБ) ?
Вложение информации в последнии биты яркости определенных пикселей сообщения.

8.Являются ли СГ системы с вложением в НЗБ необнаруживаемыми ?
Системы СГС-НЗБ легко обнаруживаются с помощью визуальной атаки, атаки первого порядка (гистограммной) и атаки второго порядка (ПВА).

9.Каковы основные преимущества и недостатки лингвистических СГ ?
Свойства всех Л-СГС:
1. Идеальная секретность.
2. В качестве ПС может выступать любой смысловой текст.
3. Низкая скорость вложения.
4. Отсутствует устойчивость к “слепой” атаке удаления вложенной информации.
5. Иногда требует участия человека – оператора.

10.Какие преимущества имеют СГ системы на основе каналов с шумом ?
1. Это единственный случай, когда можно обеспечить секретность СГС при атаке с ПС, известным в точности.
2. Выбор типа канала (BSC или гауссовский) зависит от того, в каком месте линии связи можно вкладывать и извлекать информацию.
3. Для построения СГС и атаки на нее не требуется знания статистики ПС.
4. В случае BSC количество надежно и секретно погружаемых бит ограничено, тогда как для гауссовского случая можно надежно и секретно вложить любое количество бит, однако, скорость передачи стремиться к нулю при $N \to \infty$.

11.Какие основные типы декодеров используются в СГ системах?
Информированный, легальный, слепой, корреляционный, декодер скачков.

12.Что такое “слепой” стегоанализ СГ?
Производится «обучение» идентификатора СГ по большому количеству СГ и ПС, что позволяет выработать в некотором смысле оптимальный алгоритм, принимающий решение о том, является ли представленный образец ПС или СГ

13.Перечислите основные атаки на системы СГ и ЦВЗ.
1. Визуальная атака
2. Атака первого порядка (гистограммная)
3. Атаки высоких порядков (в частности атака 2-го порядка или парный стегоанализ)

1. Обнаружение ЦВЗ в ПС (для конфиденциальных ЦВЗ).
2. Извлечение погруженного сообщения (для конфиденциальных ЦВЗ).
3. Удаление ЦВЗ без *значительного искажения* ПС.
4. Ложное погружение других ЦВЗ в ПС без его *значительного искажения*.

14.Почему в СГ системах часто используются широкополосные сигналы ?
Для защиты от атаки рандомизации НЗБ во временной или частотной области.

15.Каковы критерии эффективности систем ЦВЗ ?

- вероятность P_{fa} ошибочного обнаружения ЦВЗ (для 0-битовых ЦВЗ),
- вероятность P_m необнаружения ЦВЗ (для 0-битовых ЦВЗ),
- вероятность P_e ошибки при извлечении бита легальным декодером (для многобитовых ЦВЗ), в том числе и после естественных и преднамеренных преобразований, которые не искажают существенно ПС,
- качество ПС после погружения ЦВЗ, которое в первом приближении оценивается отношением сигнал/шум, а более точно специальными критериями и экспертами,
- скорость погружения ЦВЗ (для многобитовых ЦВЗ по отношению к объему ПС; типичная оценка в бит/отсчет аудио ПС или в бит/пиксель ПС в виде изображения).

16.В чем состоит основное отличие модели обычной системы связи и систем СГ и ЦВЗ и как это отличие используется при их построении ?

В обычной системе связи все данные передаются в открытом виде и нет скрытой информации. В СГС факт погружения не должен обнаруживаться, а защита от преднамеренного удаления не всегда необходима. ЦВЗ не обязательно должны быть необнаруживаемы, но, как правило, защищены от удалений и ложных погружений.

17.Зачем нужна “предобработка” ПС в системах ЦВЗ?

Перед вложением цвз часто производится преобразование ПС (предобработка), затем вложение ЦВЗ и выполнение обратного преобразования для формирования стеганограммы. Эти преобразования должны сохранить требуемое качество ПС и возможность последующего извлечения ЦВЗ из СГ.

Возможные виды преобразований (предобработки)

- дискретное преобразование Фурье (DFT);
- дискретное косинусное преобразование (DCT);
- дискретное преобразование Уолша (WDT);
- разложение в подходящие ряды (EAS);
- разложение в произведение матриц (EMP);

Причина целесообразности преобразований

- можно лучше учесть искажения ПС при погружении ЦВЗ;
- легче построить методы погружения и извлечения ЦВЗ устойчивые к естественным или преднамеренным преобразованиям СГ.

18.Чем отличается квантованная индексная модуляция от квантованной проективной модуляции и какие преимущества имеет последняя перед первой ?

Видно, что скалярная КИМ фактически совпадает с системой НЗБ и имеет все его недостатки. При векторной КИМ предварительно выбирается кодовая книга из двух «томов» для вложения одного бита.

Цель использования QPD: Обеспечить защиту от преднамеренного удаления ЦВЗ методом рандомизированного квантования.

19.Какие два основных типа коалиционных атак известны ?

1. При использовании одной и той же ЦВЗ для разных ПС.
2. При использовании различных ЦВЗ для одного и того же ПС(Отпечатки пальцев (Fingerprinting)).

20.Что такое модульное погружение ЦВЗ и зачем оно используется ?

Модульное погружение – это одна из техник аутентификации в СГС. Используется для исключеня необратимых искажений при декодировании. Декодирование при модульном погружении приводит к значительно большим ошибкам, чем при обычном линейном погружении.

21.В чем состоит особенность использования методов сжатия при выполнении аутентификации методом ЦВЗ ?

Невозможно выполнить обратимое погружение, если ПС не имеет избыточности. Непосредственное сжатие ПС (изображения или звука) приводит к полному их искажению для восприятия человеком. Поэтому необходимо использовать более изощренные методы погружения со сжатием без потерь, которое не искажает заметно ПС сразу после погружения аутентификаторов. Можно выбрать любой алгоритм сжатия без потерь, но наиболее предпочтительным является использование адаптивных арифметических кодов.

22.Какие атаки возможны на систему аутентификации , реализованную на основе ЦВЗ ?

23.Чем отличается точная аутентификация на основе ЦВЗ и селективная аутентификация ?

Два основных вида аутентификации в СГС:

1. Точная аутентификация (искажение даже одного бита в ПС должно обнаруживаться)

2. Селективная аутентификация (некоторые виды искажения ПС должны обнаруживаться, а другие искажения (например, добавление небольшого шума, преобразование формата и т.п.) не должны обнаруживаться).

«Парадокс» аутентификации в СГС:

при погружении аутентификатора как ЦВЗ в ПС оно неизбежно искажается, а, с другой стороны, искажение ПС приводит к невозможности его аутентификации…

Аутентификация называется селективной, если ПС считается подлинным (не измененным) при некоторых допустимых видах его преобразований (искажений) и не подлинным, если оно подвергалось недопустимым искаженным. (Выбор допустимых и недопустимых искажений зависит от конкретной задачи и условий аутентификации).