Скрытие информации

Антон Басков, OBS Group Ltd.

Основные способы применения

- Секретная передача данных
- Сокрытие данных
- Обеспечение защиты интеллектуальной собственности
- Встраивание заголовков

Проблемы

- Преимущества, которые дает хранение и передача цифровых данных, могут быть перечеркнуты легкостью воровства или модификации данных.
- Наличие у 3-х лиц (в том числе и у государственных структур) возможности не только прослушивать, но и блокировать обмен подозрительной информацией (в том числе и зашифрованными данными).

Обеспечение защиты интеллектуальной собственности

- Водные знаки / Watermarks
- Маркировка / Fingerprints & labels

Watermarks
Visible copyright messages

Цель видимого водного знака - отобразить сообщение владельца

- Документ: водяной знак “Секретно”
- Фотоархив: полупрозрачный текст “Издательство Коммерсант”
- Видео материалы: “Never copy”

Основные задачи:

- Возможность использования объекта ИС
- Стойкость (невыводимость пятна)
- Стойкость к преобразованиям (ксерокопирование, преобразование формата документа (png -> jpeg))

Watermarks
Hidden copyright messages

Цель скрытого водного знака - возможность доказать авторство документа

- Изображения: скрытая надпись с указанием автора
- Иное применение: скрытое психологическое воздействие (25 кадр, текстовый или издательский способ)

Основные задачи:

- Плохая видимость водяного знака
- Стойкость (невыводимость водяного знака)
- Повышенная устойчивость к преобразованиям документа
- “Неслучайность” – тривиальность процесса обнаружения (растяжение, увеличение, изменение контрастности)
- Возможность использования для доказательства в суде

Watermarks
Invisible copyright messages

Цель невидимого водного знака - возможность быстро идентифицировать “свои” документы в хранилище

- Казино: загнутые уголки карт
- Корпоративная сеть: поиск секретных документов на компьютерах сотрудников
- Разведка: отслеживание пути документа

Основные задачи:

- 100% невидимость водяного знака
- Стойкость (невыводимость водяного знака)
- Повышенная устойчивость к преобразованиям документа
- Высокая скорость определения своих документов

Fingerprinting

Цель - возможность быстро идентифицировать владельцев помеченных документов, аналог серийного номера

1. Распространение конфиденциальной информации в ограниченном круге лиц (поиск шпиона)
2. Скрытая идентификация (DVD или скрытый доступ к веб сайту)

Основные задачи:

- 100% невидимость водяного знака
- Стойкость (невыводимость водяного знака)
- Повышенная устойчивость к преобразованиям документа
- Высокая скорость определения владельца документа

Copyright making в целом

Общие недостатки данных систем:

- Использование только оригинальных источников данных
- Необходимость тщательного сокрытия методики установки водяного знака (в том числе разработка оригинальной методики)
- Наличие специалиста по защите интеллектуальной собственности

Возможные цели атаки:

- Возможность удаления водяного знака
- Возможность сделать водяной знак нечитаемым или изменить его содержимое
- Возможность использовать часть объекта (картинки, звука и т.п.)

Invisible watermarks & fingerprinting process

В процессе создания маркированного изображения используют исходное изображение и марку, состоящую из ключа и пометки.

Алгоритмы различают по типу процесса обнаружения маркировки (detection process):

- Private type I systems – для обнаружения пометки требуется только оригинальное изображение
- Private type II systems – требуется пометка, ключ и исходное изображение
- Semi-private systems – требуется только ключ и пометка
- Public systems – зная ключ можно получить пометку
- Public key systems – для обнаружения пометки используется общедоступный ключ

- Пометку могут обнаруживать все (заявление прав)
- Пометку может обнаруживать ограниченный круг лиц (поиск пирата)

Copyright making в целом

Практика показывает, что:

- Обычно рекомендуется не использовать готовые решения и методики, в особенности с открытым исходным кодом и от непроверенных поставщиков. Такие решения ненадежны. В отличие от шифрования лучше придумать что-либо своё.
- Задача скрытого и невидимого водяного знака – оставаться скрытым. Поэтому ни в коем случае нельзя ни публиковать сами оригиналы изображений, ни тем более предоставлять сторонним лицам сервис.
- Отсутствие понимания методики работы с объектами ИС делает применение способов защиты с помощью водных знаков невозможным.

Далее…

- Скрытая передача данных (скрытая связь)
- Хранение данных (запрятывание)
- Добавление заголовков

Скрытая передача данных

Цель - скрыть факт передачи данных

- Выжигание на лбу у гонца секретной информации
- Симпатические чернила, пунктуационные ошибки и т.п.

Основные задачи:

- Информация должна быть спрятана в контейнер с неподозрительными данными
- Затруднение идентификации отправителя и получателя
- Повышенная устойчивость к преобразованиям документа
- Определение изменений контейнера (желательно).

Скрытое хранение данных

- Цель – скрыть факт наличия данных
  - Хранение в крайне необычных местах
- Основные задачи:
  - Информация должна быть спрятана в контейнер с неподозрительными данными
  - Спецефические требования хранилища
  - Повышенная устойчивость к преобразованиям документа
  - Определение изменений контейнера (желательно).

Встраивание заголовков

Цель – хранение разнородно представленной информации в одном целом

1. Хранение на рентгеновском снимке информации о пациенте
2. Хранение на карте легенды и информации об объектах

Основные задачи:

- Удобство использования
- Защита цифровой подписью

Типичная стегосистема

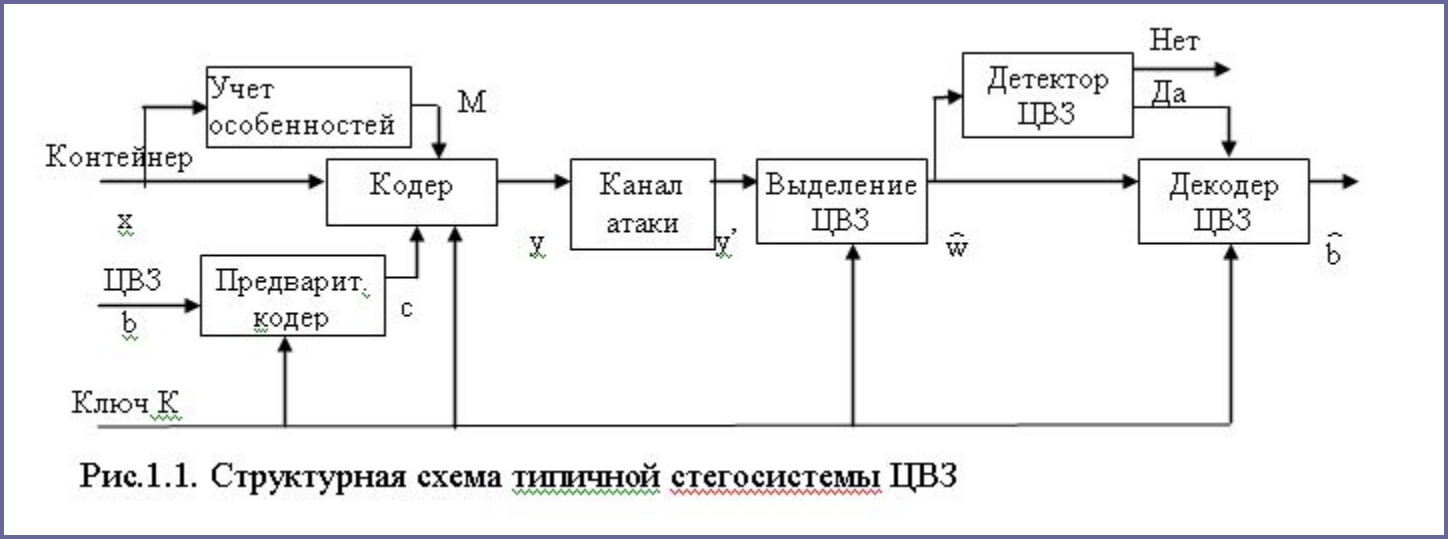


Рис.1.1. Структурная схема типичной стегосистемы ЦВЗ

Свойства идеальной системы

- Безопасность системы должна полностью определяться секретностью ключа.
- Заполненный контейнер должен быть не отличим от незаполненного.
- Наличие любого количества различных документов не дают злоумышленнику построить детектор. Даже в том случае, если он знает, что все имеющиеся у него документы одинаково маркированы (т.е. ключ и водяной знак совпадают).
- Стойкость к преобразованиям.
  - При использовании в целях проверки подлинности водяной знак должен разрушаться при недопустимых преобразованиях.
  - При использовании в целях защиты прав водяной знак не должен разрушаться при любых преобразованиях.
  - P.S. Также различают стойкость при обнаружении декодером. Например, при повороте изображения скрытый водяной знак сохраняется, но может не определятся детектором.
- Низкая вероятность ложного срабатывания детектора на чистом от цифрового водяного знака сигнале. Это может быть критично, например, при применении в DVD проигрывателе.
- Должна обеспечиваться требуемая пропускная способность (для систем скрытой связи)
- Стегосистема должна иметь приемлемую вычислительною сложность (как минимум, при реализации детектора и (желательно) декодера)
- Системы цифрового водяного знака должны позволять добавлять иные водяные знаки и (желательно) иметь возможность удаления знака правообладателем.

Атаки на системы с водяным знаком

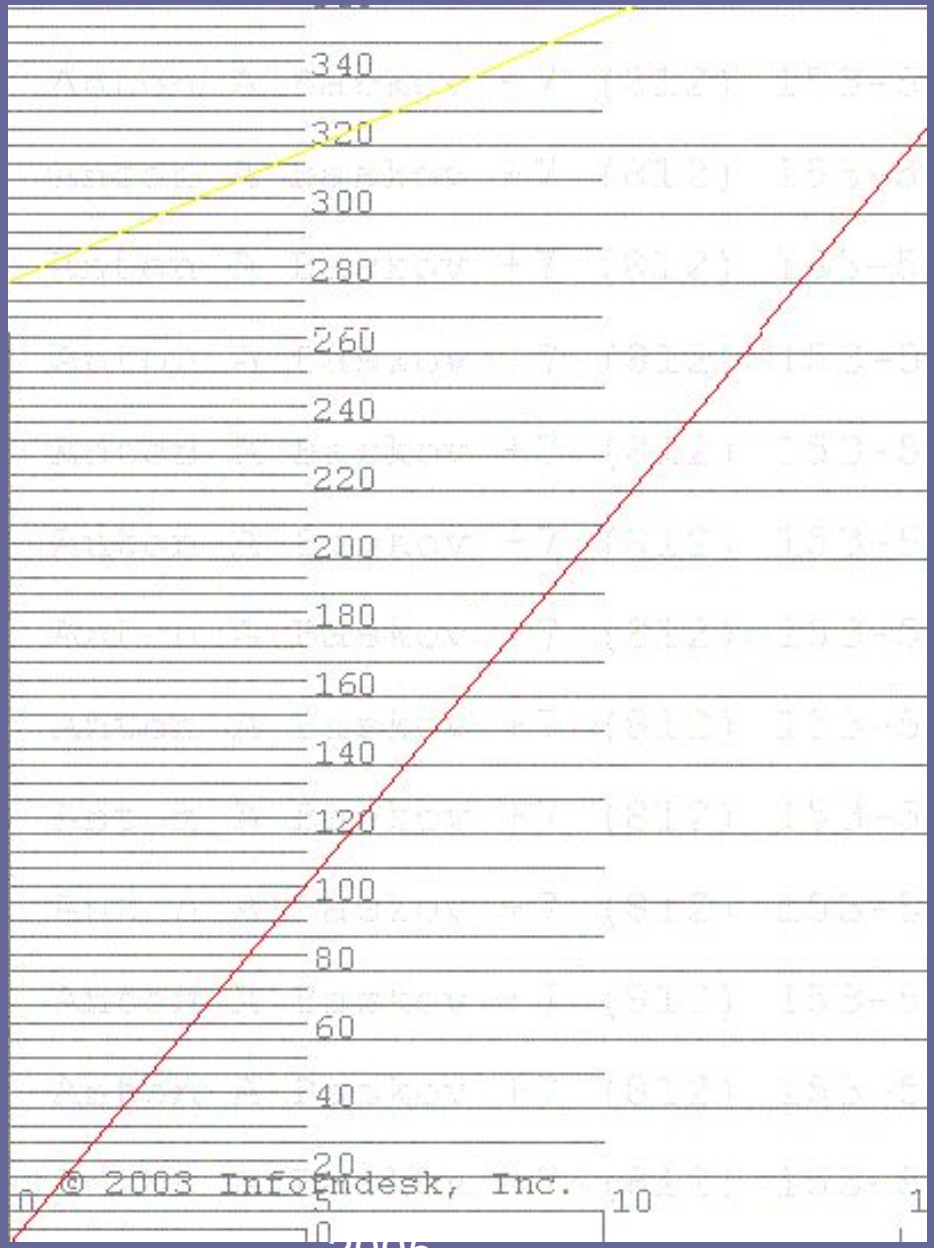
- Атаки на удаление водяного знака
- Геометрические атаки
- Криптографические атаки
- Атаки против протокола

Примеры!

Пример видимого водяного знака.

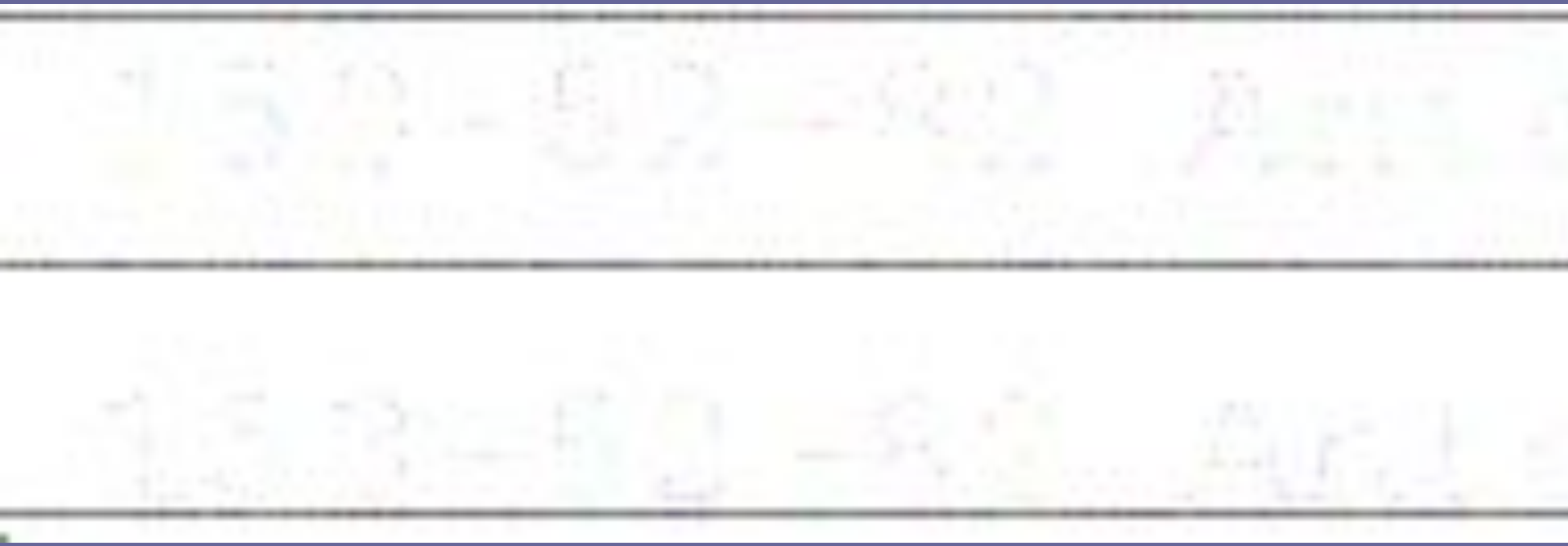
Пример видимого водяного знака.

Пример скрытого водяного знака.

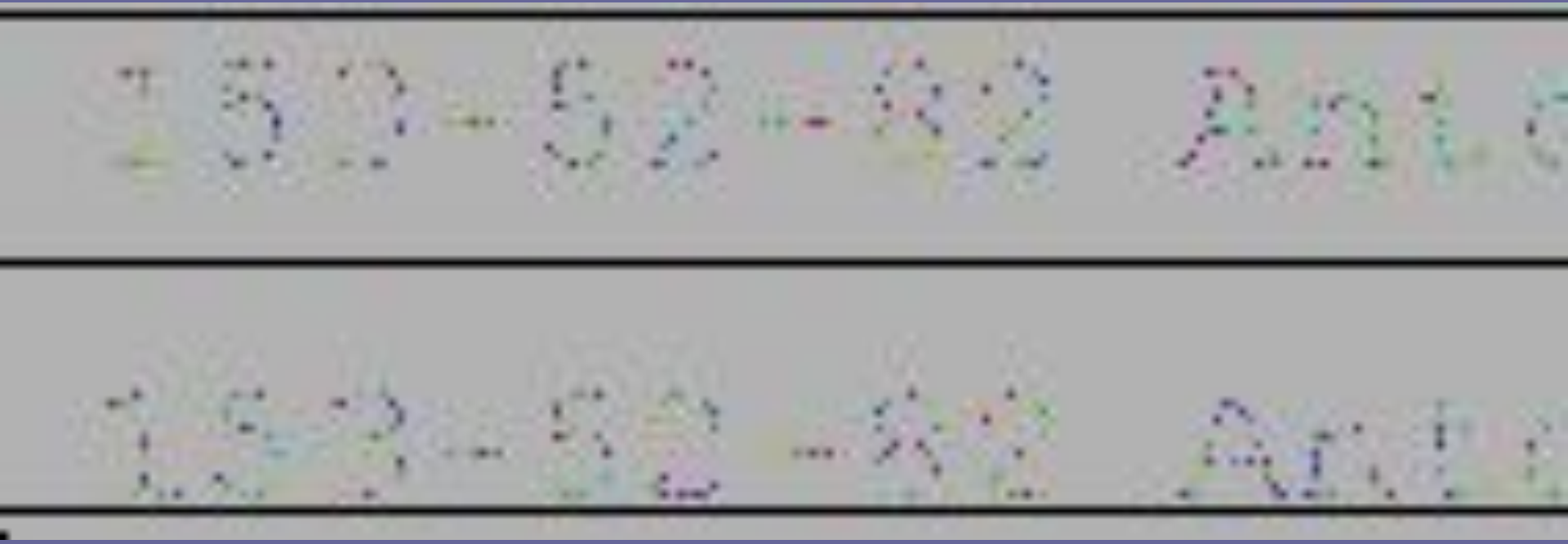


2005

Пример скрытого водяного знака.

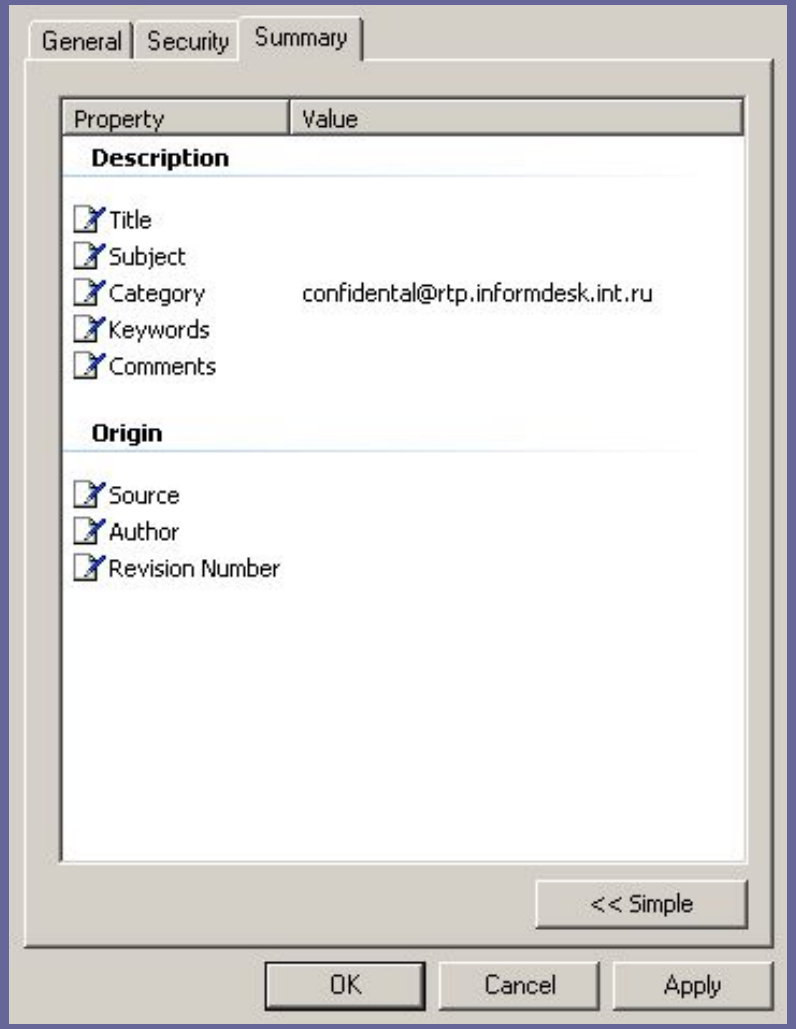


Пример скрытого водяного знака.



Пример невидимого водяного знака.

```
C:\> echo Copyright >> index.txt:copyright
```



Стеганография с открытым (общедоступным) ключом

1. Алиса генерирует на своем компьютере пару открытого и закрытого ключа.
2. Алиса пересылает открытый ключ по каналу Бобу. Эту же информацию получает и Вилли.
3. Боб предполагает, что пересланные данные есть открытый ключ Алисы. С его помощью он шифрует сообщение, состоящее из его открытого ключа для будущей связи и (возможно) краткого «приветствия». Боб пересылает это сообщение Алисе.
4. Алиса знает, что присланные данные содержат открытый ключ Боба, дешифрует их при помощи своего закрытого ключа. У узников есть вся необходимая информация для обеспечения скрытой двусторонней связи. Так как Вилли лишь Наблюдатель, то он не может никоим образом вмешаться и помешать установлению скрытой связи между Алисой и Бобом.

С использованием надсознательного канала

1. Алиса генерирует пару открытого и закрытого ключей.
2. Алиса вычисляет представительное описание контейнера, соответствующее ее открытому ключу, генерирует контейнер и пересылает его Бобу.
3. Боб извлекает из принятого контейнера открытый ключ Алисы. Он генерирует секретный ключ, шифрует его с помощью открытого ключа Алисы, находит соответствующее получившейся последовательности описание контейнера, генерирует контейнер и пересылает его Алисе.
4. Алиса и Боб теперь могут обмениваться сообщениями, встраиваемыми в контейнер с использованием этого ключа.

Вилли в результате перехвата канала может получить открытый ключ Алисы и зашифрованный этим ключом секретный ключ Боба. Не зная закрытого ключа Алисы он не сможет получить значение секретного ключа.

Источники информации

1. “Цифровая стеганография”, Вадим Геннадьевич Грибунин.
2. IEEE Information Hiding (http://www.petitcolas.net/fabien/publications/ieee99-infohiding.pdf)

The End!

Saint Petersburg University User Group