Лекция 3. Модели стойкости асимметричных шифров. Криптографические примитивы: хэш-функции, ГПП

Косолапов Ю.В.

ЮФУ

21 сентября 2020 г.

Содержание

Модели стойкости асимметричных систем

Модели стойкости асимметричных систем

- Неразличимость шифртекста на основе подобранного открытого текста (IND-CPA)

Модели стойкости асимметричных систем

- Неразличимость шифртекста на основе подобранного открытого текста (IND-CPA)
- Неразличимость шифртекста на основе подобранного шифртекста (IND-CCA1/IND-CCA2)

Криптографическая хэш-функция

Предположим, что имеется отображение $h : D \to \{0,1\}^n$, D — область определения функции (domain). Возможны следующшие условия на h

Криптографическая хэш-функция

Предположим, что имеется отображение $h : D \to \{0,1\}^n$, D — область определения функции (domain). Возможны следующшие условия на h

1. $D = \{0,1\}^n$

Криптографическая хэш-функция

Предположим, что имеется отображение $h : D \to \{0,1\}^n$, D — область определения функции (domain). Возможны следующшие условия на h

1. $D = \{0,1\}^n$
2. $D = \{0,1\}^{n+k}$, $k > 0$

Криптографическая хэш-функция

Предположим, что имеется отображение $h : D \to \{0,1\}^n$, D — область определения функции (domain). Возможны следующшие условия на h

1. $D = \{0,1\}^n$
2. $D = \{0,1\}^{n+k}$, $k > 0$
3. $D = \{0,1\}^*$.

Криптографическая хэш-функция

Предположим, что имеется отображение $h : D \to \{0,1\}^n$, D — область определения функции (domain). Возможны следующшие условия на h

1. $D = \{0,1\}^n$
2. $D = \{0,1\}^{n+k}$, $k > 0$
3. $D = \{0,1\}^*$.
4. Для всех $x \in D$ значение $h(x)$ вычисляется легко.

Криптографическая хэш-функция

Предположим, что имеется отображение $h : D \to \{0,1\}^n$, D — область определения функции (domain). Возможны следующшие условия на h

1. $D = \{0,1\}^n$
2. $D = \{0,1\}^{n+k}$, $k > 0$
3. $D = \{0,1\}^*$.
4. Для всех $x \in D$ значение $h(x)$ вычисляется легко.
5. Почти для всех $y \in \mathrm{Im}(h)$ вычислительно сложно найти такой x, что $h(x) = y$ (**однонаправленность**).

Криптографическая хэш-функция

Предположим, что имеется отображение $h : D \to \{0,1\}^n$, D — область определения функции (domain). Возможны следующшие условия на h

1. $D = \{0,1\}^n$
2. $D = \{0,1\}^{n+k}$, $k > 0$
3. $D = \{0,1\}^*$.
4. Для всех $x \in D$ значение $h(x)$ вычисляется легко.
5. Почти для всех $y \in \mathrm{Im}(h)$ вычислительно сложно найти такой x, что $h(x) = y$ (**однонаправленность**).
6. Для заданного $x \in D$ вычислительно сложно найти $x' \neq x$, такой, что $h(x) = h(x')$ (**слабая устойчивость к коллизиям**).

Криптографическая хэш-функция

Предположим, что имеется отображение $h : D \to \{0,1\}^n$, D — область определения функции (domain). Возможны следующшие условия на h

1. $D = \{0,1\}^n$
2. $D = \{0,1\}^{n+k}$, $k > 0$
3. $D = \{0,1\}^*$.
4. Для всех $x \in D$ значение $h(x)$ вычисляется легко.
5. Почти для всех $y \in \mathrm{Im}(h)$ вычислительно сложно найти такой x, что $h(x) = y$ (**однонаправленность**).
6. Для заданного $x \in D$ вычислительно сложно найти $x' \neq x$, такой, что $h(x) = h(x')$ (**слабая устойчивость к коллизиям**).
7. Вычислительно сложно найти любую пару $x' \neq x$, такую, что $h(x) = h(x')$ (**сильная устойчивость к коллизиям**).

Криптографическая хэш-функция

Классификация отображений:

Криптографическая хэш-функция

Классификация отображений:

- Если 1, 4 и 5, то это **односторонняя** функция;

Криптографическая хэш-функция

Классификация отображений:

- Если 1, 4 и 5, то это **односторонняя** функция;
- Если 2, 4, 5, 6, 7, то это **сжимающая** функция;

Криптографическая хэш-функция

Классификация отображений:

- Если 1, 4 и 5, то это **односторонняя** функция;
- Если 2, 4, 5, 6, 7, то это **сжимающая** функция;
- Если 3, 4, 5, 6, то это одностороння **хэш**-функция;

Криптографическая хэш-функция

Классификация отображений:

- Если 1, 4 и 5, то это **односторонняя** функция;
- Если 2, 4, 5, 6, 7, то это **сжимающая** функция;
- Если 3, 4, 5, 6, то это одностороння **хэш**-функция;
- Если 3, 4, 5, 6, 7, то это **криптографическая хэш**-функция.

Построение криптографический хэш-функций

Построение криптографический хэш-функций

- Пусть $g : \{0,1\}^{n+k} \to \{0,1\}^n$ — сжимающая функция (в качестве такой функции может выступать симметричнное шифрование);

Построение криптографический хэш-функций

- Пусть $g : \{0,1\}^{n+k} \to \{0,1\}^n$ — сжимающая функция (в качестве такой функции может выступать симметричнное шифрование);
- Пусть $g : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ (например, алгоритм блочного шифрования);

Построение криптографический хэш-функций

- Пусть $g : \{0,1\}^{n+k} \to \{0,1\}^n$ — сжимающая функция (в качестве такой функции может выступать симметричнное шифрование);
- Пусть $g : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ (например, алгоритм блочного шифрования);
- Хэшируемый текст $\mathbf{X}$ представляется в виде последовательности k-битных блоков:

$$\mathbf{X} = (\mathbf{x}_1, ..., \mathbf{x}_m);$$

Построение криптографический хэш-функций

- Пусть $g : \{0,1\}^{n+k} \to \{0,1\}^n$ — сжимающая функция (в качестве такой функции может выступать симметричнное шифрование);
- Пусть $g : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ (например, алгоритм блочного шифрования);
- Хэшируемый текст $\mathbf{X}$ представляется в виде последовательности k-битных блоков:

$$\mathbf{X} = (\mathbf{x}_1, ..., \mathbf{x}_m);$$

- Выполняется последовательность действий:

Построение криптографический хэш-функций

- Пусть $g : \{0,1\}^{n+k} \to \{0,1\}^n$ — сжимающая функция (в качестве такой функции может выступать симметричнное шифрование);
- Пусть $g : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ (например, алгоритм блочного шифрования);
- Хэшируемый текст $\mathbf{X}$ представляется в виде последовательности k-битных блоков:

$$\mathbf{X} = (\mathbf{x}_1, ..., \mathbf{x}_m);$$

- Выполняется последовательность действий:
  - $h_0 := IV$ (начальный вектор длины n, известен всем, прописан в документации)

Построение криптографический хэш-функций

- Пусть $g : \{0,1\}^{n+k} \to \{0,1\}^n$ — сжимающая функция (в качестве такой функции может выступать симметричнное шифрование);
- Пусть $g : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ (например, алгоритм блочного шифрования);
- Хэшируемый текст $\mathbf{X}$ представляется в виде последовательности k-битных блоков:

$$\mathbf{X} = (\mathbf{x}_1, ..., \mathbf{x}_m);$$

- Выполняется последовательность действий:
  - $h_0 := IV$ (начальный вектор длины n, известен всем, прописан в документации)
  - $h_1 := g(h_0, \mathbf{x}_1)$

Построение криптографический хэш-функций

- Пусть $g : \{0,1\}^{n+k} \to \{0,1\}^n$ — сжимающая функция (в качестве такой функции может выступать симметричнное шифрование);
- Пусть $g : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ (например, алгоритм блочного шифрования);
- Хэшируемый текст $\mathbf{X}$ представляется в виде последовательности k-битных блоков:

$$\mathbf{X} = (\mathbf{x}_1, ..., \mathbf{x}_m);$$

- Выполняется последовательность действий:
  - $h_0 := IV$ (начальный вектор длины n, известен всем, прописан в документации)
  - $h_1 := g(h_0, \mathbf{x}_1)$
  - $h_2 := g(h_1, \mathbf{x}_2)$

Построение криптографический хэш-функций

- Пусть $g : \{0,1\}^{n+k} \to \{0,1\}^n$ — сжимающая функция (в качестве такой функции может выступать симметричнное шифрование);
- Пусть $g : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ (например, алгоритм блочного шифрования);
- Хэшируемый текст $\mathbf{X}$ представляется в виде последовательности k-битных блоков:

$$\mathbf{X} = (\mathbf{x}_1, ..., \mathbf{x}_m);$$

- Выполняется последовательность действий:
  - $h_0 := IV$ (начальный вектор длины n, известен всем, прописан в документации)
  - $h_1 := g(h_0, \mathbf{x}_1)$
  - $h_2 := g(h_1, \mathbf{x}_2)$
  - ...

Построение криптографический хэш-функций

- Пусть $g : \{0,1\}^{n+k} \to \{0,1\}^n$ — сжимающая функция (в качестве такой функции может выступать симметричнное шифрование);
- Пусть $g : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ (например, алгоритм блочного шифрования);
- Хэшируемый текст $\mathbf{X}$ представляется в виде последовательности k-битных блоков:

$$\mathbf{X} = (\mathbf{x}_1, ..., \mathbf{x}_m);$$

- Выполняется последовательность действий:
  - $h_0 := IV$ (начальный вектор длины n, известен всем, прописан в документации)
  - $h_1 := g(h_0, \mathbf{x}_1)$
  - $h_2 := g(h_1, \mathbf{x}_2)$
  - ...
  - $h_m := g(h_{m-1}, \mathbf{x}_m)$

Построение криптографический хэш-функций

- Пусть $g : \{0,1\}^{n+k} \to \{0,1\}^n$ — сжимающая функция (в качестве такой функции может выступать симметричнное шифрование);
- Пусть $g : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ (например, алгоритм блочного шифрования);
- Хэшируемый текст $\mathbf{X}$ представляется в виде последовательности k-битных блоков:

$$\mathbf{X} = (\mathbf{x}_1, ..., \mathbf{x}_m);$$

- Выполняется последовательность действий:
  - $h_0 := IV$ (начальный вектор длины n, известен всем, прописан в документации)
  - $h_1 := g(h_0, \mathbf{x}_1)$
  - $h_2 := g(h_1, \mathbf{x}_2)$
  - ...
  - $h_m := g(h_{m-1}, \mathbf{x}_m)$
  - $h(\mathbf{X}) := h_m$.

Виды «случайностей»

Виды «случайностей»

Определение „Словарь криптографических терминов“ под редакцией Б.А. Погорелова и В.Н. Сачкова.

Истинно случайная последовательность – последовательность, порожденная недетерминированным физическим устройством или процессом. Такая последовательность непредсказуема и невоспроизводима.

Виды «случайностей»

Определение „Словарь криптографических терминов“ под редакцией Б.А. Погорелова и В.Н. Сачкова.

Истинно случайная последовательность – последовательность, порожденная недетерминированным физическим устройством или процессом. Такая последовательность непредсказуема и невоспроизводима.

Определение

Последовательность случайная идеальна – последовательность, являющаяся реализацией последовательности независимых случайных величин, имеющих равномерное распределение на заданном конечном алфавите.

Виды «случайностей»

Определение „Словарь криптографических терминов“ под редакцией Б.А. Погорелова и В.Н. Сачкова.

Истинно случайная последовательность – последовательность, порожденная недетерминированным физическим устройством или процессом. Такая последовательность непредсказуема и невоспроизводима.

Определение

Последовательность случайная идеальна – последовательность, являющаяся реализацией последовательности независимых случайных величин, имеющих равномерное распределение на заданном конечном алфавите.

Определение

Последовательность псевдослучайная – последовательность, порожденная детерминированным устройством или программой (генератором псевдослучайных последовательностейб ГПП).

Генератор псевдослучайных чисел

Определение

Генератор последовательностей псевдослучайных криптографически сильный — ГПП, который порождает псевдослучайную последовательность, неотличимую эффективно (с полиномиальной сложностью) статистическими тестами от идеальной случайной последовательности.

Генератор псевдослучайных чисел

Определение

Генератор последовательностей псевдослучайных криптографически сильный — ГПП, который порождает псевдослучайную последовательность, неотличимую эффективно (с полиномиальной сложностью) статистическими тестами от идеальной случайной последовательности.

Статистические тесты NIST SP 800-22:

- Частотный побитовый тест
- Частотный блочный тест
- Тест на последовательность одинаковых битов
- ...

В NIST SP 800-22 порядка 15 видов тестов. Есть и другие тесты: «стопка книг» и его вариации, например.

Генератор псевдослучайных последовательностей (криптографически сильный)

Используются

Генератор псевдослучайных последовательностей (криптографически сильный)

Используются

- для генерации долговременных секретных ключ симметричных шифров;

Генератор псевдослучайных последовательностей (криптографически сильный)

Используются

- для генерации долговременных секретных ключ симметричных шифров;
- для генерации долговременных секретных ключ асимметричных шифров;

Генератор псевдослучайных последовательностей (криптографически сильный)

Используются

- для генерации долговременных секретных ключ симметричных шифров;
- для генерации долговременных секретных ключ асимметричных шифров;
- для генерации сессионных ключей (в асимметричных системах эти ключи могут иметь разный формат: ср. систему Эль-Гамаля с системой Мак-Элиса);

Генератор псевдослучайных последовательностей (криптографически сильный)

Используются

- для генерации долговременных секретных ключ симметричных шифров;
- для генерации долговременных секретных ключ асимметричных шифров;
- для генерации сессионных ключей (в асимметричных системах эти ключи могут иметь разный формат: ср. систему Эль-Гамаля с системой Мак-Элиса);
- для генерации запросов в протоколах типа запрос-ответ.

Генератор псевдослучайных последовательностей (криптографически сильный)

Используются

- для генерации долговременных секретных ключ симметричных шифров;
- для генерации долговременных секретных ключ асимметричных шифров;
- для генерации сессионных ключей (в асимметричных системах эти ключи могут иметь разный формат: ср. систему Эль-Гамаля с системой Мак-Элиса);
- для генерации запросов в протоколах типа запрос-ответ.
- ...

Требования к криптографически сильным ГПП

Требования к криптографически сильным ГПП

- Простота генерации;

Требования к криптографически сильным ГПП

- Простота генерации;
- Непредсказуемость полиномиальными алгоритмами генерируемых битов (= неотличимость от идеальной случайной последовательности)

Способы построения ГПП

На основе симметричных шифров. Например, используя режим шифрования OFB (Output Feedback):

$$\mathbf{e}_1 = E_{\mathbf{k}}(\mathbf{0}), \mathbf{e}_2 = E_{\mathbf{k}}(\mathbf{e}_1), ..., \mathbf{e}_t = E_{\mathbf{k}}(\mathbf{e}_t - 1), ...$$

ПП – это битовое представление последовательсноти векторов:

$$\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_t, ...,$$

Здесь $\mathbf{k}$ — это инициализация генератора (аналог входного параметра в srand()).

Способы построения ГПП

На основе симметричных шифров. Например, используя режим шифрования OFB (Output Feedback):

$$\mathbf{e}_1 = E_{\mathbf{k}}(\mathbf{0}), \mathbf{e}_2 = E_{\mathbf{k}}(\mathbf{e}_1), ..., \mathbf{e}_t = E_{\mathbf{k}}(\mathbf{e}_t - 1), ...$$

ПП – это битовое представление последовательсноти векторов:

$$\mathbf{e}_1, \mathbf{e}_2, ..., \mathbf{e}_t, ...,$$

Здесь $\mathbf{k}$ — это инициализация генератора (аналог входного параметра в srand()).
Есть и другие способы построения ГПП: на основе регистров сдвига с линейной обратной связью, на основе трудных предикатов односторонних функций (hard core predicate)

Способы построения ГПП

Есть и другие способы построения ГПП:

Способы построения ГПП

Есть и другие способы построения ГПП:

- на основе регистров сдвига с линейной обратной связью (РСЛОС);

Способы построения ГПП

Есть и другие способы построения ГПП:

- на основе регистров сдвига с линейной обратной связью (РСЛОС);
- на основе трудных предикатов односторонних функций (hard core predicate).

Способы построения ГПП

Есть и другие способы построения ГПП:

- на основе регистров сдвига с линейной обратной связью (РСЛОС);
- на основе трудных предикатов односторонних функций (hard core predicate).

Нестрогое определение трудного предиката

Предикат $B(x)$ является трудным для функции $f(x)$, если по элементу x значение $B(x)$ вычисляется легко, а по $f(x)$ — вычислительно сложно.

Способы построения ГПП

Есть и другие способы построения ГПП:

- на основе регистров сдвига с линейной обратной связью (РСЛОС);
- на основе трудных предикатов односторонних функций (hard core predicate).

Нестрогое определение трудного предиката

Предикат $B(x)$ является трудным для функции $f(x)$, если по элементу x значение $B(x)$ вычисляется легко, а по $f(x)$ — вычислительно сложно.

Example

$f(x) \equiv x^2 \mathrm{mod} n$, где $n = pq$, $B(x) =$ „x–нечетное“.

Способы построения ГПП

Есть и другие способы построения ГПП:

- на основе регистров сдвига с линейной обратной связью (РСЛОС);
- на основе трудных предикатов односторонних функций (hard core predicate).

Нестрогое определение трудного предиката

Предикат $B(x)$ является трудным для функции $f(x)$, если по элементу x значение $B(x)$ вычисляется легко, а по $f(x)$ — вычислительно сложно.

Example

$f(x) \equiv x^2 \mathrm{mod} n$, где $n = pq$, $B(x) =$ „x–нечетное“.

Непредсказуемая последовательность

$$B(x), B(f^{-1}(x)), B(f^{-1}(f^{-1}(x))), ...$$

Заключение

Спасибо за внимание!