Лекция 2. Классификация криптографических протоколов. Криптографические примитивы: симметричное и асимметричное шифрование

Косолапов Ю.В.

ЮФУ

14 сентября 2020 г.

Содержание

Классификация

Классификация

- по числу участников: двусторонний, трехсторонний (и т.п.), многосторонний;

Классификация

- по числу участников: двусторонний, трехсторонний (и т.п.), многосторонний;
- по целевому назначению: зависит от *цели*;

Классификация

- по числу участников: двусторонний, трехсторонний (и т.п.), многосторонний;
- по целевому назначению: зависит от *цели*;
- примитивные/прикладные;

Классификация

- по числу участников: двусторонний, трехсторонний (и т.п.), многосторонний;
- по целевому назначению: зависит от *цели*;
- примитивные/прикладные;
- по типу используемых криптографических систем: симметричные, асимметричные;

Классификация

- по числу участников: двусторонний, трехсторонний (и т.п.), многосторонний;
- по целевому назначению: зависит от *цели*;
- примитивные/прикладные;
- по типу используемых криптографических систем: симметричные, асимметричные;
- по способу функционирования: интерактивные/неинтерактивные, однопроходный/двух-/трех- и т.д. проходный, протоколы с арбитром, с доверенной третьей стороной (ТЗР).

Криптографические методы

Методы:

Криптографические методы

Методы:

- симметричное шифрование;

Криптографические методы

Методы:

- симметричное шифрование;
- асимметричное шифрование;

Криптографические методы

Методы:

- симметричное шифрование;
- асимметричное шифрование;
- криптографическая хэш-функция;

Криптографические методы

Методы:

- симметричное шифрование;
- асимметричное шифрование;
- криптографическая хэш-функция;
- генератор псевдослучайных чисел;

Криптографические методы

Методы:

- симметричное шифрование;
- асимметричное шифрование;
- криптографическая хэш-функция;
- генератор псевдослучайных чисел;
- цифровая подпись;

Криптографические методы

Методы:

- симметричное шифрование;
- асимметричное шифрование;
- криптографическая хэш-функция;
- генератор псевдослучайных чисел;
- цифровая подпись;
- гомоморфное шифрование.

Определение шифра

Определение

$$(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

Определение шифра

Определение

$$(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

- $\mathcal{X} = \{\mathbf{x}_1, ..., \mathbf{x}_M\}$ — множество шифруемых (открытых) текстов;

Определение шифра

Определение

$$(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

- $\mathcal{X} = \{\mathbf{x}_1, ..., \mathbf{x}_M\}$ — множество шифруемых (открытых) текстов;
- $\mathcal{Y} = \{\mathbf{y}_1, ..., \mathbf{y}_P\}$ — множество шифртекстов текстов;

Определение шифра

Определение

$$(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

- $\mathcal{X} = \{\mathbf{x}_1, ..., \mathbf{x}_M\}$ — множество шифруемых (открытых) текстов;
- $\mathcal{Y} = \{\mathbf{y}_1, ..., \mathbf{y}_P\}$ — множество шифртекстов текстов;
- $\mathcal{K} = \{\mathbf{k}_1, ..., \mathbf{k}_N\}$ — множество ключей.

Определение шифра

Определение

$$(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

- $\mathcal{X} = \{\mathbf{x}_1, ..., \mathbf{x}_M\}$ — множество шифруемых (открытых) текстов;
- $\mathcal{Y} = \{\mathbf{y}_1, ..., \mathbf{y}_P\}$ — множество шифртекстов текстов;
- $\mathcal{K} = \{\mathbf{k}_1, ..., \mathbf{k}_N\}$ — множество ключей.
- $\mathcal{E} = \{E_{\mathbf{k}} : \mathbf{k} \in \mathcal{K}\}$ — правила шифрования;

Определение шифра

Определение

$$(\mathcal{X}, \mathcal{Y}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

- $\mathcal{X} = \{\mathbf{x}_1, ..., \mathbf{x}_M\}$ — множество шифруемых (открытых) текстов;
- $\mathcal{Y} = \{\mathbf{y}_1, ..., \mathbf{y}_P\}$ — множество шифртекстов текстов;
- $\mathcal{K} = \{\mathbf{k}_1, ..., \mathbf{k}_N\}$ — множество ключей.
- $\mathcal{E} = \{E_{\mathbf{k}} : \mathbf{k} \in \mathcal{K}\}$ — правила шифрования;
- $\mathcal{D} = \{D_{\mathbf{k}} : \mathbf{k} \in \mathcal{K}\}$ — правила расшифрования;

Определение симметричного шифра

Определение

Симметричный шифр — это такой шифр, в котором при шифровании и расшифровании используется один и тот же ключ (либо по ключу шифрования можно «просто» найти ключ расшифрования).

Определение симметричного шифра

Определение

Симметричный шифр — это такой шифр, в котором при шифровании и расшифровании используется один и тот же ключ (либо по ключу шифрования можно «просто» найти ключ расшифрования).

Примеры симметричных шифров:

- $\texttt{GOST28147} - 89$ (Магма в ГОСТ Р 34.12-2015), $\mathcal{X} = \mathcal{Y} = \{0,1\}^{64}$, $\mathcal{K} = \{0,1\}^{256}$;

Определение симметричного шифра

Определение

Симметричный шифр — это такой шифр, в котором при шифровании и расшифровании используется один и тот же ключ (либо по ключу шифрования можно «просто» найти ключ расшифрования).

Примеры симметричных шифров:

- `GOST28147 − 89` (Магма в ГОСТ Р 34.12-2015), $\mathcal{X} = \mathcal{Y} = \{0,1\}^{64}$, $\mathcal{K} = \{0,1\}^{256}$;
- `Kuznechik` (Кузнечик в ГОСТ Р 34.12-2015), $\mathcal{X} = \mathcal{Y} = \{0,1\}^{128}$, $\mathcal{K} = \{0,1\}^{256}$;

Определение симметричного шифра

Определение

Симметричный шифр — это такой шифр, в котором при шифровании и расшифровании используется один и тот же ключ (либо по ключу шифрования можно «просто» найти ключ расшифрования).

Примеры симметричных шифров:

- `GOST28147 – 89` (Магма в ГОСТ Р 34.12-2015), $\mathcal{X} = \mathcal{Y} = \{0,1\}^{64}$, $\mathcal{K} = \{0,1\}^{256}$;
- `Kuznechik` (Кузнечик в ГОСТ Р 34.12-2015), $\mathcal{X} = \mathcal{Y} = \{0,1\}^{128}$, $\mathcal{K} = \{0,1\}^{256}$;
- `AES`, $\mathcal{X} = \mathcal{Y} = \{0,1\}^{128}$, $\mathcal{K} = \{0,1\}^{128}, \{0,1\}^{192}, \{0,1\}^{256}$.

Определение асимметричного шифра

Определение

Асимметричный шифр — это такой шифр, в котором при шифровании и расшифровании используются разные ключи: публичный и секретный. При этом по публичному ключу **сложно** найти секретный.

Определение асимметричного шифра

Определение

Асимметричный шифр — это такой шифр, в котором при шифровании и расшифровании используются разные ключи: публичный и секретный. При этом по публичному ключу **сложно** найти секретный.

Примеры асимметричных шифров:

- RSA, $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_n$, $\mathcal{K}_{pub} = \mathbb{Z}_{\phi(n)}$, $\mathcal{K}_{sec} = \mathbb{Z}_{\phi(n)}$, $n = pq$, p и q — простые, $|p|_2, |q|_2 \geqslant 2048$ (основана на сложности факторизации целых чисел);

Определение асимметричного шифра

Определение

Асимметричный шифр — это такой шифр, в котором при шифровании и расшифровании используются разные ключи: публичный и секретный. При этом по публичному ключу **сложно** найти секретный.

Примеры асимметричных шифров:

- RSA, $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_n$, $\mathcal{K}_{pub} = \mathbb{Z}_{\phi(n)}$, $\mathcal{K}_{sec} = \mathbb{Z}_{\phi(n)}$, $n = pq$, p и q — простые, $|p|_2, |q|_2 \geqslant 2048$ (основана на сложности факторизации целых чисел);
- Система Эль-Гамаля, $\mathcal{X} = \mathbb{Z}_p$, $\mathcal{Y} = \mathbb{Z}_p \times \mathbb{Z}_p$, $\mathcal{K}_{pub} = \mathbb{Z}_p$, $\mathcal{K}_{sec} = \mathbb{Z}_p \backslash \{0\}$, p – простое, $|p|_2 \geqslant 2048$ (основана на сложности вычисления дискретного логарифма в конечной группе);

Определение асимметричного шифра

Определение

Асимметричный шифр — это такой шифр, в котором при шифровании и расшифровании используются разные ключи: публичный и секретный. При этом по публичному ключу **сложно** найти секретный.

Примеры асимметричных шифров:

- RSA, $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_n$, $\mathcal{K}_{pub} = \mathbb{Z}_{\phi(n)}$, $\mathcal{K}_{sec} = \mathbb{Z}_{\phi(n)}$, $n = pq$, p и q — простые, $|p|_2, |q|_2 \geqslant 2048$ (основана на сложности факторизации целых чисел);
- Система Эль-Гамаля, $\mathcal{X} = \mathbb{Z}_p$, $\mathcal{Y} = \mathbb{Z}_p \times \mathbb{Z}_p$, $\mathcal{K}_{pub} = \mathbb{Z}_p$, $\mathcal{K}_{sec} = \mathbb{Z}_p \backslash \{0\}$, p – простое, $|p|_2 \geqslant 2048$ (основана на сложности вычисления дискретного логарифма в конечной группе);
- Мак-Элиса, $\mathcal{X} = \{0,1\}^k$, $\mathcal{Y} = \{0,1\}^n$, $\mathcal{K}_{pub}$ — подмножество $(k \times n)$-матриц полного ранга, $\mathcal{K}_{sec}$ — множество троек матриц (S, G, Q) специального вида, $k \geqslant 5413$, $n \geqslant 6960$, (основана на сложности декодирования кода *общего положения*).

Примеры асимметричных шифров

- RSA, $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_n$, $\mathcal{K}_{pub} = \mathbb{Z}_{\phi(n)}$, $\mathcal{K}_{sec} = \mathbb{Z}_{\phi(n)}$, $n = pq$, p и q — простые, $|p|_2, |q|_2 \geqslant 2048$ (основана на сложности факторизации целых чисел);

Примеры асимметричных шифров

- RSA, $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_n$, $\mathcal{K}_{pub} = \mathbb{Z}_{\phi(n)}$, $\mathcal{K}_{sec} = \mathbb{Z}_{\phi(n)}$, $n = pq$, p и q — простые, $|p|_2, |q|_2 \geqslant 2048$ (основана на сложности факторизации целых чисел);
- Система Эль-Гамаля, $\mathcal{X} = \mathbb{Z}_p$, $\mathcal{Y} = \mathbb{Z}_p \times \mathbb{Z}_p$, $\mathcal{K}_{pub} = \mathbb{Z}_p$, $\mathcal{K}_{sec} = \mathbb{Z}_p \backslash \{0\}$, p – простое, $|p|_2 \geqslant 2048$ (основана на сложности вычисления дискретного логарифма в конечной группе);

Примеры асимметричных шифров

- RSA, $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_n$, $\mathcal{K}_{pub} = \mathbb{Z}_{\phi(n)}$, $\mathcal{K}_{sec} = \mathbb{Z}_{\phi(n)}$, $n = pq$, p и q — простые, $|p|_2, |q|_2 \geqslant 2048$ (основана на сложности факторизации целых чисел);
- Система Эль-Гамаля, $\mathcal{X} = \mathbb{Z}_p$, $\mathcal{Y} = \mathbb{Z}_p \times \mathbb{Z}_p$, $\mathcal{K}_{pub} = \mathbb{Z}_p$, $\mathcal{K}_{sec} = \mathbb{Z}_p \backslash \{0\}$, p – простое, $|p|_2 \geqslant 2048$ (основана на сложности вычисления дискретного логарифма в конечной группе);
- Мак-Элиса, $\mathcal{X} = \{0,1\}^k$, $\mathcal{Y} = \{0,1\}^n$, $\mathcal{K}_{pub}$ — подмножество $(k \times n)$-матриц полного ранга, $\mathcal{K}_{sec}$ — множество троек матриц (S, G, Q) специального вида, $k \geqslant 5413$, $n \geqslant 6960$, (основана на сложности декодирования кода *общего положения*).

Подробнее об RSA

Построение ключей

Подробнее об RSA

Построение ключей

- Случайно выбираются два больших простых числа p и q;

Подробнее об RSA

Построение ключей

- Случайно выбираются два больших простых числа p и q;
- Вычисляются $n = pq$, $\phi(n) = (p-1)(q-1)$;

Подробнее об RSA

Построение ключей

- Случайно выбираются два больших простых числа p и q;
- Вычисляются $n = pq$, $\phi(n) = (p-1)(q-1)$;
- Выбирается $1 < e < \phi(n)$, взаимно простое с $\phi(n)$ (для однозначности расшифрования);

Подробнее об RSA

Построение ключей

- Случайно выбираются два больших простых числа p и q;
- Вычисляются $n = pq$, $\phi(n) = (p-1)(q-1)$;
- Выбирается $1 < e < \phi(n)$, взаимно простое с $\phi(n)$ (для однозначности расшифрования);
- Из сравнения $de \equiv 1(\mathrm{mod}(\phi(n)))$ находится d;

Подробнее об RSA

Построение ключей

- Случайно выбираются два больших простых числа p и q;
- Вычисляются $n = pq$, $\phi(n) = (p-1)(q-1)$;
- Выбирается $1 < e < \phi(n)$, взаимно простое с $\phi(n)$ (для однозначности расшифрования);
- Из сравнения $de \equiv 1(\mathrm{mod}(\phi(n)))$ находится d;
- e – публичный ключ, d – секретный ключ.

Подробнее об RSA

Шифрование и расшифрование.

Подробнее об RSA

Шифрование и расшифрование.

- Шифрование сообщения $m \in \mathbb{Z}_n$: $m^e (\mathrm{mod} n) = C$;

Подробнее об RSA

Шифрование и расшифрование.

- Шифрование сообщения $m \in \mathbb{Z}_n$: $m^e (\mathrm{mod} n) = C$;
- Расшифрование: $C^d (\mathrm{mod} n) = m^{ed} (\mathrm{mod} n) = m^{ed} (\mathrm{mod} n) = m^{t \cdot \phi(n)+1} (\mathrm{mod} n) = m^{t \cdot \phi(n)} m (\mathrm{mod} n) = m$;

Подробнее о схеме Эль-Гамаля

Построение ключей

Подробнее о схеме Эль-Гамаля

Построение ключей

- Выбирается случайное простое число p, $|p|_2 \geqslant 2048$

Подробнее о схеме Эль-Гамаля

Построение ключей

- Выбирается случайное простое число p, $|p|_2 \geqslant 2048$
- Находится порождающий элемент g группы $\mathbb{Z}_p^*$

Подробнее о схеме Эль-Гамаля

Построение ключей

- Выбирается случайное простое число p, $|p|_2 \geqslant 2048$
- Находится порождающий элемент g группы $\mathbb{Z}_p^*$
- Выбирается случайное число $x \in \mathbb{Z}_p$, $x \neq 0$

Подробнее о схеме Эль-Гамаля

Построение ключей

- Выбирается случайное простое число p, $|p|_2 \geqslant 2048$
- Находится порождающий элемент g группы $\mathbb{Z}_p^*$
- Выбирается случайное число $x \in \mathbb{Z}_p$, $x \neq 0$
- Вычисляется $y = g^x (\mathrm{mod} p)$

Подробнее о схеме Эль-Гамаля

Построение ключей

- Выбирается случайное простое число p, $|p|_2 \geqslant 2048$
- Находится порождающий элемент g группы $\mathbb{Z}_p^*$
- Выбирается случайное число $x \in \mathbb{Z}_p$, $x \neq 0$
- Вычисляется $y = g^x (\mathrm{mod} p)$
- y – открытый ключ, x – закрытый ключ.

Подробнее о схеме Эль-Гамаля

Шифрование сообщения $m \in \mathbb{Z}_p$ с помощью открытого ключа y.

Подробнее о схеме Эль-Гамаля

Шифрование сообщения $m \in \mathbb{Z}_p$ с помощью открытого ключа y.

- Выбирается случайное число $k \in \mathbb{Z}_p$, $k \neq 0$,

Подробнее о схеме Эль-Гамаля

Шифрование сообщения $m \in \mathbb{Z}_p$ с помощью открытого ключа y.

- Выбирается случайное число $k \in \mathbb{Z}_p$, $k \neq 0$,
- Вычисляются два значения: $a = g^k (\mathrm{mod} p)$, $b = y^k m (\mathrm{mod} p)$;

Подробнее о схеме Эль-Гамаля

Шифрование сообщения $m \in \mathbb{Z}_p$ с помощью открытого ключа y.

- Выбирается случайное число $k \in \mathbb{Z}_p$, $k \neq 0$,
- Вычисляются два значения: $a = g^k (\mathrm{mod} p)$, $b = y^k m (\mathrm{mod} p)$;
- Пара (a, b) является шифртекстом.

Подробнее о схеме Эль-Гамаля

Расшифрование шифртекста (a, b) с помощью секретного ключа x:

$$\frac{b}{a^x}(\mathrm{mod} p) = \frac{y^k m}{(g^k)^x}(\mathrm{mod} p) = \frac{(g^x)^k m}{(g^k)^x}(\mathrm{mod} p) = m(\mathrm{mod} p).$$

Подробнее о схеме Мак-Элиса

Построение ключей:

Подробнее о схеме Мак-Элиса

Построение ключей:

- Выбирается порождающая матрица G_C для $[n, k, d]_q$-кода C (код позволяет исправить до $t = \lceil \frac{d-1}{2} \rceil$ ошибок, для кода должен быть известен быстрый алгоритм декодирования $\mathrm{Dec} : \mathbb{F}_q^n \to \mathbb{F}_q^k$);

Подробнее о схеме Мак-Элиса

Построение ключей:

- Выбирается порождающая матрица G_C для $[n, k, d]_q$-кода C (код позволяет исправить до $t = \lceil \frac{d-1}{2} \rceil$ ошибок, для кода должен быть известен быстрый алгоритм декодирования $\mathrm{Dec} : \mathbb{F}_q^n \to \mathbb{F}_q^k$);
- Выбирается невырожденная $(k \times k)$-матрица S

Подробнее о схеме Мак-Элиса

Построение ключей:

- Выбирается порождающая матрица G_C для $[n, k, d]_q$-кода C (код позволяет исправить до $t = \lceil \frac{d-1}{2} \rceil$ ошибок, для кода должен быть известен быстрый алгоритм декодирования $\mathrm{Dec} : \mathbb{F}_q^n \to \mathbb{F}_q^k$);
- Выбирается невырожденная $(k \times k)$-матрица S
- Выбирается перестановочная $(n \times n)$-матрица Q

Подробнее о схеме Мак-Элиса

Построение ключей:

- Выбирается порождающая матрица G_C для $[n, k, d]_q$-кода C (код позволяет исправить до $t = \lceil \frac{d-1}{2} \rceil$ ошибок, для кода должен быть известен быстрый алгоритм декодирования $\mathrm{Dec} : \mathbb{F}_q^n \to \mathbb{F}_q^k$);
- Выбирается невырожденная $(k \times k)$-матрица S
- Выбирается перестановочная $(n \times n)$-матрица Q
- Находится матрица $G = S \cdot G_C \cdot Q$.
- Пара (G, t) — открытый ключ, тройка (S, C, Q) — секретный ключ.

Подробнее о схеме Мак-Элиса

Шифрование сообщения $\mathbf{m}$:

$$\mathbf{m}G + \mathbf{e} = \mathbf{c}, \mathrm{wt}(\mathbf{e}) \leqslant t.$$

$\mathrm{wt}(\mathbf{e}) -$ число ненулевых координат в векторе $\mathbf{e}$(вес Хэмминга).

Подробнее о схеме Мак-Элиса

Расшифрование шифртекста $\mathbf{c}$:

Подробнее о схеме Мак-Элиса

Расшифрование шифртекста $\mathbf{c}$:

- $$\begin{aligned}\mathbf{c}Q^{-1} &= (\mathbf{m}G + \mathbf{e})Q^{-1} = \mathbf{m}SG_CQQ^{-1} + \mathbf{e}Q^{-1} \\ &= \mathbf{m}SG_C + \mathbf{e}' = \mathbf{m}'G_C + \mathbf{e}', (\mathbf{m}' = \mathbf{m}S, \mathbf{e}' = \mathbf{e}Q^{-1}).\end{aligned}$$

Подробнее о схеме Мак-Элиса

Расшифрование шифртекста $\mathbf{c}$:

- $$\begin{aligned}\mathbf{c}Q^{-1} &= (\mathbf{m}G + \mathbf{e})Q^{-1} = \mathbf{m}SG_CQQ^{-1} + \mathbf{e}Q^{-1} \\ &= \mathbf{m}SG_C + \mathbf{e}' = \mathbf{m}'G_C + \mathbf{e}', (\mathbf{m}' = \mathbf{m}S, \mathbf{e}' = \mathbf{e}Q^{-1}).\end{aligned}$$

- $$\mathbf{m}' = \mathrm{Dec}(\mathbf{c}Q^{-1})$$

Подробнее о схеме Мак-Элиса

Расшифрование шифртекста $\mathbf{c}$:

- $$\begin{aligned}\mathbf{c}Q^{-1} &= (\mathbf{m}G + \mathbf{e})Q^{-1} = \mathbf{m}SG_CQQ^{-1} + \mathbf{e}Q^{-1} \\ &= \mathbf{m}SG_C + \mathbf{e}' = \mathbf{m}'G_C + \mathbf{e}', (\mathbf{m}' = \mathbf{m}S, \mathbf{e}' = \mathbf{e}Q^{-1}).\end{aligned}$$

- $$\mathbf{m}' = \mathrm{Dec}(\mathbf{c}Q^{-1})$$

- $$\mathbf{m} = \mathbf{m}'S^{-1}.$$

Заключение

Спасибо за внимание!