2 Классические криптосистемы

2.1 Алфавит

Рассмотрим примеры классических (докомпьютерных) криптосистем или, как их еще называют, шифров. Пусть используется алфавит из m символов. Каждому символу поставим в соответствие числа от 0 до $m-1$. Например, русский алфавит «оцифруем» следующим образом:

А $= 0$	К $= 11$	Х $= 22$
Б $= 1$	Л $= 12$	Ц $= 23$
В $= 2$	М $= 13$	Ч $= 24$
Г $= 3$	Н $= 14$	Ш $= 25$
Д $= 4$	О $= 15$	Щ $= 26$
Е $= 5$	П $= 16$	Ъ $= 27$
Ё $= 6$	Р $= 17$	Ы $= 28$
Ж $= 7$	С $= 18$	Ь $= 29$
З $= 8$	Т $= 19$	Э $= 30$
И $= 9$	У $= 20$	Ю $= 31$
Й $= 10$	Ф $= 21$	Я $= 32$

Для дальнейшего изложения нам потребуются некоторые факты из элементарной теории чисел и алгебры.

A. Число $a \in \mathbb{Z}$ *делит* $b \in \mathbb{Z}$ (пишем $a \mid b$), если $b = ak$, $k \in \mathbb{Z}$.

Через $a \mod m$ обозначаем остаток от деления a на $m \in \mathbb{N}$.

Числа a и b *сравнимы* по модулю m (пишем $a \equiv b \pmod{m}$), если $m \mid a - b$.

Н.о.д. чисел a и b обозначается через (a, b). Числа a и b *взаимно просты*, если $(a, b) = 1$.

Н.о.к. чисел a и b обозначается через $[a, b]$.

Упражнение 2.1. $(0, 0)$ — ? □

B. *Кольцом* $\langle R, +, * \rangle$ называется множество R с двумя бинарными операциями $+$ и $*$ такими, что

1) $\langle R, + \rangle$ — абелева группа;
2) операция $*$ ассоциативна, т. е. $(a * b) * c = a * (b * c)$ для всех $a, b, c \in R$;
3) выполняются законы дистрибутивности:

$$a * (b + c) = a * b + a * c, \quad (a + b) * c = a * c + b * c, \quad a, b, c \in R.$$

C. Множество $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ с операциями сложения и умножения по модулю m является кольцом (классов вычетов целых чисел по модулю m).

Упражнение 2.2. Подтвердить утверждение C. □

Для построения криптосистем естественно воспользоваться алфавитом $\mathbb{Z}_m$ и операциями сложения и умножения для его символов.

2.2 Шифр сдвига

Шифр использует аддитивную группу $\langle \mathbb{Z}_m, + \rangle$ кольца $\mathbb{Z}_m$:

$$C = \langle \mathbb{Z}_m, \mathbb{Z}_m, \mathbb{Z}_m, E, D \rangle,$$

где $E_K(X) = X + K$, $D_K(Y) = Y - K$.

Гай Юлий Цезарь использовал шифр сдвига с фиксированным ключом $K = 3$ и старым латинским алфавитом из 23 символов (без J, U, W).

Пример 2.1. Зашифруем сообщение НЕДОВЕРЯЙВИКТОРУ на ключе Г $= 3$. Получим сообщение РЗЖСЕЗУВМЕЛНХСУЦ. □

2.3 Аффинный шифр

Теорема 2.1. Сравнение $ax \equiv b \pmod{m}$ имеет единственное решение относительно $x \in \mathbb{Z}_m$ при любом целом b тогда и только тогда, когда $(a, m) = 1$.

Доказательство. Необходимость. Если, от противного, $(a, m) = d > 1$, то сравнение $ax \equiv 0 \pmod{m}$ имеет по крайней мере два различных решения $x_1 = 0$ и $x_2 = m/d$. Противоречие.

Достаточность. Предположим, что $(a, m) = 1$ и заявленное сравнение имеет два решения $x_1, x_2 \in \mathbb{Z}_m$. Тогда

$$ax_1 \equiv ax_2 \pmod{m} \Rightarrow a(x_1 - x_2) \equiv 0 \pmod{m} \Rightarrow m \mid a(x_1 - x_2) \overset{(a,m)=1}{\Rightarrow} m \mid (x_1 - x_2) \Rightarrow x_1 \equiv x_2 \pmod{m}$$

и $x_1 = x_2$. □

Теорема означает следующее. Если $(a, m) = 1$, то число a *обратимо* по модулю m, т. е. найдется $x \in \mathbb{Z}_m$ такое, что $ax \equiv 1 \pmod{m}$. Такое x называется *мультипликативно обратным* к a элементом и обозначается через $a^{-1} \bmod m$.

Пусть $\mathbb{Z}_m^*$ — множество всех обратимых $\bmod m$ элементов $\mathbb{Z}_m$. *Функция Эйлера* $\varphi(m)$ определяется правилом $\varphi(m) = |\mathbb{Z}_m^*|$. Другими словами, $\varphi(m)$ есть количество чисел от 0 до $m - 1$, взаимно простых с m.

Для определения значений $\varphi(m)$ можно использовать два свойства:

1) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ для простых p;

2) если $(a, b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$.

Отсюда $\varphi(m) = m \prod_{p|m}(1 - 1/p)$. Действительно, пусть $m = \prod_{i=1}^k p_i^{\alpha_i}$, где p_i — различные простые. Тогда

$$\varphi(m) = \prod_{i=1}^k \varphi(p_i^{\alpha_i}) = \prod_{i=1}^k p_i^{\alpha_i}(1 - 1/p_i) = m \prod_{p|m}(1 - 1/p).$$

Теорема 2.2 (Эйлера). Если $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Доказательство. В силу предыдущей теоремы отображение $\mathbb{Z}_m^* \to \mathbb{Z}_m^*$, $x \mapsto ax$ является биекцией. Поэтому

$$\prod_{x \in \mathbb{Z}_m^*} x = \prod_{x \in \mathbb{Z}_m^*} (ax) = a^{\varphi(m)} \prod_{x \in \mathbb{Z}_m^*} x$$

(вычисления $\bmod m$), откуда следует требуемое сравнение. □

Следствием теоремы Эйлера является малая теорема Ферма:

Теорема 2.3 (Ферма). Если p — простое, p не делит a, то $a^{p-1} \equiv 1 \pmod{p}$.

Теорему Эйлера можно использовать для нахождения мультипликативно обратных:

$$a^{-1} \bmod m = a^{\varphi(m)-1} \bmod m.$$

Пример 2.2. Найдем $14^{-1} \bmod 33$. Во-первых, определим $\varphi(33) = \varphi(3)\varphi(11) = 20$. Вычислим степени:

$$14^2 = 196 \equiv -2 \pmod{33}, \quad 14^4 = (-2)^2 \equiv 4 \pmod{33}, \quad 14^8 = 4^2 \equiv 16 \pmod{33}, \quad 14^{16} = 16^2 = 256 \equiv 25 \pmod{33}.$$

Теперь

$$14^{\varphi(33)-1} = 14^{19} = 14 \cdot 14^2 \cdot 14^{16} \equiv 14 \cdot (-2) \cdot 25 \equiv 5 \cdot 25 \equiv 26 \pmod{33}.$$

Таким образом, $14^{-1} \bmod 33 = 26$. □

Замечание 2.1. Вычисление мультипликативно обратных можно упростить, используя теорему Кармайкла: $(a, m) = 1 \Rightarrow a^{\lambda(m)} \equiv 1 \pmod{m}$. Здесь $\lambda(m)$ — функция Кармайкла:

1) $\lambda(p^\alpha) = \varphi(p^\alpha)$, если $p \neq 2$ или $p = 2$ и $\alpha \leqslant 2$;

2) $\lambda(2^\alpha) = \frac{1}{2}\varphi(2^\alpha)$, $\alpha \geqslant 3$;

3) $(a, b) = 1 \Rightarrow \lambda(ab) = [\lambda(a), \lambda(b)]$.

Например, $\lambda(33) = [\lambda(3), \lambda(11)] = [2, 10] = 10$. Поэтому $14^{-1} \bmod 33 = 14^{\lambda(33)-1} \bmod 33 = 14^9 \bmod 33$. □

Вернемся к шифру сдвига. Недостатком шифра является малое число ключей. Мощность ключевого пространства можно повысить, если задействовать еще и мультипликативную группу $\langle \mathbb{Z}_m^*, *\rangle$:

$$C = \langle \mathbb{Z}_m^* \times \mathbb{Z}_m, \mathbb{Z}_m, \mathbb{Z}_m, E, D\rangle,$$

где $E_K(X) = aX + b$, $D_K(Y) = a^{-1}(Y - b)$. Теперь $|\mathcal{K}| = \varphi(m)m$.

Пример 2.3. Зашифруем сообщение `НЕДОВЕРЯЙВИКТОРУ` на ключе (`Н` $= 14$, `О` $= 15$). Получим сообщение `МТЕЪЙТХБЦЙИДРЪХЮ`. □

Упражнение 2.3. Найти $14^{-1} \bmod 33$ и расшифровать последнее сообщение. □

2.4 Шифр простой замены

Ключевое пространство предыдущего шифра можно довести до максимально возможного (при условии, что ключи не эквивалентны) — до $m!$. Для этого в качестве ключа можно использовать всевозможные подстановки на $\mathbb{Z}_m$:

$$C = \langle S(\mathbb{Z}_m), \mathbb{Z}_m, \mathbb{Z}_m, E, D\rangle,$$

где $E_K(X) = K(X)$, $D_K(Y) = K^{-1}(Y)$.

Пример 2.4. Используем подстановку

$$\begin{pmatrix} \texttt{АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ} \\ \texttt{СЪЕШЬЩЁЭТИХМЯГКФРАНЦУЗБЛОДВЫПЙЖЧЮ} \end{pmatrix}.$$

На таком ключе сообщение `НЕДОВЕРЯЙВИКТОРУ` будет преобразовано в `КЩЬФЕ....`

Для определения подстановки использована панграмма (слово, в котором встречаются все буквы алфавита): «Съешь ещё этих мягких французских булок, да выпей же чаю». □

Пример 2.5 (RFC 2410). Стандарт Интернет RFC 2410 (The NULL Encryption Algorithm and Its Use With IPsec) определяет криптосистему NULL. Преобразования зашифрования — тождественные подстановки! Описание криптосистемы содержит шуточные элементы, но в целом введение криптосистемы вполне логично: с ее помощью удобно описывать случаи передачи данных в открытом виде. □

2.5 Шифр Хилла

Рассмотрим матрицу над кольцом $\mathbb{Z}_m$:

$$K = \begin{pmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{pmatrix}.$$

Пусть $\det K = K_{11}K_{22} - K_{12}K_{21} \in \mathbb{Z}_m^*$. Тогда определена обратная матрица:

$$K^{-1} = (\det K)^{-1} \begin{pmatrix} K_{22} & -K_{12} \\ -K_{21} & K_{11} \end{pmatrix}.$$

Шифр Хилла — первый пример блочной криптосистемы с длиной блока $n > 1$:

$$\mathcal{K} = \{K\colon \det K \in \mathbb{Z}_m^*\}, \quad \mathcal{X} = \mathcal{Y} = \mathbb{Z}_m^2, \quad E_K(x_1x_2) = (x_1, x_2)K, \quad D_K(y_1y_2) = (y_1, y_2)K^{-1}.$$

Пример 2.6. Зашифруем сообщение `НЕДОВЕРЯЙВИКТОРУ` на ключе $\begin{pmatrix} \texttt{К} & \texttt{Л} \\ \texttt{Ч} & \texttt{Ю} \end{pmatrix}$. Получим `???`. □

2.6 Шифр перестановки

Шифр перестановки является еще одним примером блочной криптосистемы с длиной блока $n > 1$:

$$\mathcal{K} = S(\{1, 2, \ldots, n\}), \quad E_K(x_1 x_2 \ldots x_n) = x_{K^{-1}(1)} x_{K^{-1}(2)} \ldots x_{K^{-1}(n)}, \quad D_K(y_1 y_2 \ldots y_n) = y_{K(1)} y_{K(2)} \ldots y_{K(n)}.$$

Пример 2.7. Используя расположение букв в слове `ПРИВЕТ`, получим перестановку $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 1 & 2 & 6 \end{pmatrix}$. На этом ключе зашифруем сообщение `НЕДОВЕРЯЙВИКТОРУ`, дописав к нему незначащие символы `Ж`, `З`. Получим `ОВДНЕЕ...`. □

2.7 Шифр Виженера

Шифр был описан в XVI веке французским послом в Риме Блезом де Виженером в книге «Трактат о шифрах и тайнописи».[1] Шифр признавался надежным в течение 400 лет. Шифр Виженера называют также шифром периодического лозунга. $\Sigma = \mathbb{Z}_m$, $\mathcal{K} = \Sigma^* \setminus \{\perp\}$, $\gamma = KK \ldots K$ (конкатенация нужного числа экземпляров), $E_{\gamma_i}(x_i) = x_i + \gamma_i$, $D_{\gamma_i}(y_i) = y_i - \gamma_i$.

Пример 2.8. Зашифруем сообщение `НЕДОВЕРЯЙВИКТОРУ` на ключе `КЛЮЧ`. Получим сообщение `ШРВЁМРОЦФНЖВЭЪОК`. □

[1] На самом деле Виженер не придумал, а просто описал уже известный шифр. Интересно, что в его трактате есть такие слова: «Все вещи в мире представляют собой шифр. Вся природа является просто шифром и секретным письмом».