Математические и компьютерные основы защиты информации

Лекция 2

Антон Николаевич Гайдук | УНИВЕР

vk.com/gaidukedu

16 февраля 2023 г.

Содержание дисциплины

Раздел I Введение

- Тема 1. Введение. История. Основные понятия.

Раздел II Симметричная криптография

- Тема 2 Классические шифры.
- Тема 3 Поточные алгоритмы шифрования.
- Тема 4 Блочные алгоритмы шифрования.

- Тема 5 Функции хэширования.
- Тема 6 Математические методы криптоанализа.

Раздел III Асимметричная криптография

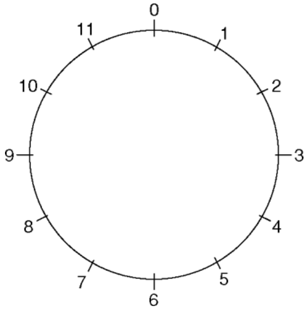
- Тема 7 Протокол Диффи-Хэллмана.
- Тема 8 Криптосистемы с открытым ключом.
- Тема 9 Электронная цифровая подпись.

Тема 2 Классические шифры

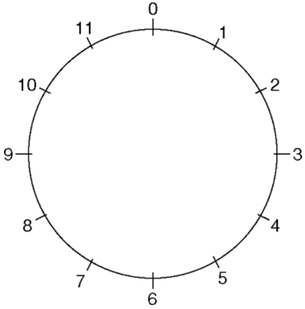
- модулярная арифметика
- понятие группы и кольца
- шифры перестановки
- шифры подстановки
- шифр сдвига
- аффинный шифр
- шифр простой замены
- шифр Виженера
- шифр Хилла

Модулярная арифметика

Модулярная арифметика



Модулярная арифметика



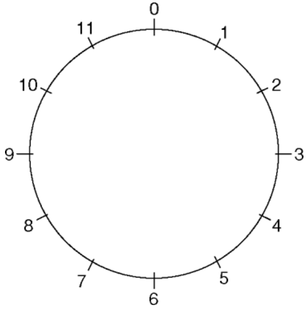
Теорема

Пусть $a \in \mathbb{Z}$ — целое, $m \in \mathbb{N}$ — натуральное, тогда существуют такие однозначно определенные $q, r \in \mathbb{Z}$, $0 \leqslant r < m$, что

$$a = mq + r.$$

r (remainder) — остаток от a по модулю m.

Модулярная арифметика



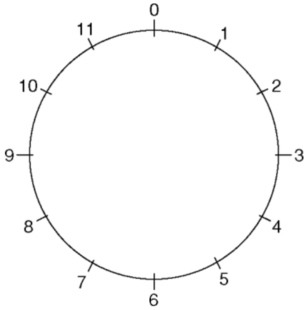
Определение

Целые числа a и b сравнимы (конгруэтны) по модулю m

$$a \equiv b \pmod{m},$$

если $m|(a-b)$ или (равносильно) числа a и b имеют одинаковые остатки при делении на m.

Модулярная арифметика



Теорема

Целые числа a и b сравнимы по модулю m тогда и только тогда, когда $\exists k \in \mathbb{Z}$ такое, что
$$a = b + km.$$

Модулярная арифметика: $(\mathrm{mod}\ )$ vs $\mod$

Обозначение **mod** имеет разный смысл:

- $a \equiv b \pmod m$ — определяет бинарное отношение,
- $a \mod m = b$ — определяет отображение (функцию) из множества целых чисел в множество целых чисел.

Теорема

Пусть $a, b \in \mathbb{Z}$ и $m \in \mathbb{N}$, тогда $a \equiv b \pmod m$ тогда и только тогда, когда

$$a \mod m = b \mod m.$$

Модулярная арифметика

- Проверочная цифра в номере ISBN вычисляется по модулю 10.
- $14 \equiv 2 \pmod{12} \Leftrightarrow 12|(14-2)$, $\{\dots, -22, -10, 2, 14, 26, \dots\}$
- $11 \equiv -1 \pmod{3} \Leftrightarrow 3|(11-(-1))$, $\{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$

$\equiv$ является бинарным отношением эквивалентности:

- рефлексивность: $a \equiv a$,
- симметричность: $a \equiv b \Rightarrow b \equiv a$,
- транзитивность: $a \equiv b \equiv c \Rightarrow a \equiv c$.

Числа, сравнимы по модулю m образуют класс вычетов по модулю m. Поскольку это отношение является бинарным отношением эквивалентности, то имеем разбиение на классы эквивалентности (классы вычетов). Всего m классов:

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\},$$
$$\mathbb{Z}_m = \{0, 1, \dots, m-1\}.$$

Модулярная арифметика

Выполняются законы

- коммутативности: $a + b \equiv b + a \pmod{m}$,
  $ab \equiv ba \pmod{m}$,
- ассоциативности: $(a + b) + c \equiv a + (b + c) \pmod{m}$,
  $(ab)c \equiv a(bc) \pmod{m}$,
- дистрибутивности: $(b + c)a \equiv ba + ca \pmod{m}$.

Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то

- $a \pm c \equiv b \pm d \pmod{m}$,
- $ac \equiv bd \pmod{m}$,
- $a^t \equiv b^t \pmod{m}$.

$$\underbrace{1 + \cdots + 1}_{m} \equiv 0 \pmod{m}.$$

Модулярная арифметика

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}.$$

Таблица сложения по модулю 6

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Таблица умножения по модулю 6

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Модулярная арифметика

При вычислении выражения по модулю m, можно заменять промежуточные результаты, на значения сравнимые с модулем m:

- $a \pm b \pmod m \equiv (a \pmod m \pm b \pmod m) \pmod m$,
- $ab \pmod m \equiv ((a \pmod m)(b \pmod m)) \pmod m$,
- $a(b \pm c) \pmod m \equiv ((ab) \pmod m \pm (ac) \pmod m) \pmod m$.

Модулярная арифметика

При вычислении выражения по модулю m, можно заменять промежуточные результаты, на значения сравнимые с модулем m:

- $a \pm b \pmod m \equiv (a \pmod m \pm b \pmod m) \pmod m$,
- $ab \pmod m \equiv ((a \pmod m)(b \pmod m)) \pmod m$,
- $a(b \pm c) \pmod m \equiv ((ab) \pmod m \pm (ac) \pmod m) \pmod m$.

Признаки делимости целых чисел

Модулярная арифметика

При вычислении выражения по модулю m, можно заменять промежуточные результаты, на значения сравнимые с модулем m:

- $a \pm b \pmod m \equiv (a \pmod m \pm b \pmod m) \pmod m$,
- $ab \pmod m \equiv ((a \pmod m)(b \pmod m)) \pmod m$,
- $a(b \pm c) \pmod m \equiv ((ab) \pmod m \pm (ac) \pmod m) \pmod m$.

Делится ли $4^n + n(n^2+5) - 4$ на 3 ?

Модулярная арифметика

При вычислении выражения по модулю m, можно заменять промежуточные результаты, на значения сравнимые с модулем m:

- $a \pm b \pmod{m} \equiv (a \pmod{m} \pm b \pmod{m}) \pmod{m}$,
- $ab \pmod{m} \equiv ((a \pmod{m})(b \pmod{m})) \pmod{m}$,
- $a(b \pm c) \pmod{m} \equiv ((ab) \pmod{m} \pm (ac) \pmod{m}) \pmod{m}$.

Эффективное выполнение операции возведения в степень.

Найти $10^{19} \pmod{21}$

$$10^{19} \equiv 10 \cdot 10^{18} \equiv 10 \cdot 100^9 \equiv [100 \equiv -5 \pmod{21}] \equiv 10 \cdot (-5)^9 \equiv$$
$$\equiv 50 \cdot (-5)^8 \equiv [-50 \equiv -8 \pmod{21}] \equiv -8 \cdot 25^4 \pmod{21} \equiv [25 \equiv 4 \pmod{21}]$$
$$\equiv (-8) \cdot 4^4 \equiv (-8) \cdot 16^2 \equiv (-8) \cdot (-5)^2 \equiv (-8) \cdot 4 \equiv -32 \equiv 10 \pmod{21}.$$

Модулярная арифметика

Алгоритм вычисления $a^d \pmod m$

1. Представить d в двоичной системе счисления:
$$d = d_0 2^k + d_1 2^{k-1} + \dots + d_{k-1} 2 + d_k, \qquad d_0 = 1.$$
2. Положить $a_0 = a$, для $j = \overline{1, k}$ вычислить a_j:
$$a_j = a_{j-1}^2 a^{d_j} \pmod m$$
3. Вернуть a_k.

Обоснование
$d = (\dots((d_0 2 + d_1)2 + d_2)2 + \dots + d_{k-1})2 + d_k =$
$2(2(\dots 2(2d_0 + d_1) + \dots + d_{k-2}) + d_{k-1}) + d_k$.

$$218 = 2^7 + 2^6 + 2^4 + 2^3 + 2.$$

$$3^{218} = 3^{2^7+2^6+2^4+2^3+2} = 3^{2(2(2(2(2(2(2+1)+0)+1)+1)+0)+1)+0}$$

Модулярная арифметика

$10 \equiv 6 \pmod 4$, но $5 \not\equiv 3 \pmod 4$.

Если $at \equiv bt \pmod{mt}$, то $a \equiv b \pmod m$.

Если $at \equiv bt \pmod m$ и $\gcd(t, m) = 1$, то $a \equiv b \pmod m$.

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$$

Если сравнение $ax \equiv 1 \pmod m$ имеет единственное решение над множеством $\mathbb{Z}_m$, то данное решение обозначается $a^{-1} \pmod m$ и называется обратным к a по модулю m.

a^{-1} — это целое число из $\mathbb{Z}_m$.

$5^{-1} \pmod{17} = 7$, т.к $7 \cdot 5 = 35 \equiv 1 \pmod{17}$.

Модулярная арифметика

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}.$$

Таблица умножения по модулю 7

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	$\boxed{1}$	2	3	4	5	6
2	0	2	4	6	$\boxed{1}$	3	5
3	0	3	6	2	5	$\boxed{1}$	4
4	0	4	$\boxed{1}$	5	2	6	3
5	0	5	3	$\boxed{1}$	6	4	2
6	0	6	5	4	3	2	$\boxed{1}$

Модулярная арифметика

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 7, 8, 9, 10, 11\}.$$

Таблица умножения по модулю 12

$\cdot$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	$\boxed{1}$	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	$\boxed{1}$	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	$\boxed{1}$	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	$\boxed{1}$

Теорема

Сравнение $ax \equiv 1 \pmod{m}$ имеет единственное решение тогда и только тогда, когда $\gcd(a, m) = 1$.

Понятие группы

Группой называется непустое множество G с алгебраической операцией $*$ на нем, для которой выполняются три следующие аксиомы.

1. Операция $*$ ассоциативна, т. е. для любых $a, b, c \in G$
$$a * (b * c) = (a * b) * c.$$
2. В G имеется единичный элемент e такой, что для любого $a \in G$
$$a * e = e * a = a.$$
3. Для каждого $a \in G$ существует обратный элемент $a^{-1} \in G$ такой, что
$$a * a^{-1} = a^{-1} * a = e.$$

Если дополнительно группа удовлетворяет четвертой аксиоме:

4. Для любых $a, b \in G$
$$a * b = b * a,$$

то группа называется абелевой (или коммутативной).

Пример группы: группа подстановок

Обозначим через $\mathcal{X}$ конечное множество, а его элементы обозначим через $1, 2, \ldots, n$.

Определение

Подстановка — биективное преобразование множества $\mathcal{X}$ ($\sigma : \mathcal{X} \to \mathcal{X}$).

Легко видеть, что подстановки образуют группу относительно операции композиции отображений. Эта группа называется симметрической группой n-й степени и обозначается через S_n или $S(\mathcal{X})$. Нетрудно показать, что $|S_n| = n!$.

Группа S_3 состоит из шести подстановок:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Условимся при вычислении композиции подстановок $\sigma_1\sigma_2$ выполнять отображения справа налево, т. е. сначала отображение σ_2, а затем σ_1.

Пример группы: группа подстановок

Обратная подстановка

$$\forall x \in \mathcal{X} \qquad \sigma^{-1}\sigma(x) = x.$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$$

Переворот:

$$\begin{pmatrix} 3 & 1 & 5 & 2 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

Сортировка по первой строке:

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$$

Кольцо

Кольцом называется множество R с двумя бинарными операциями, обозначаемыми символами $+$ и $\cdot$, такими, что:

1. R — абелева группа относительно операции $+$;
2. операция умножения ассоциативна, т.е. для всех $a, b, c \in R$ $(ab)c = a(bc)$;
3. выполняются законы дистрибутивности, т.е. для всех $a, b, c \in R$

$$a(b+c) = ab + ac \text{ и } (b+c)a = ba + ca.$$

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

Модулярная арифметика

Множество $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m | \gcd(a, m) = 1\}$ вместе с операцией умножения по модулю m, называется мультипликативной группой кольца вычетов по модулю m.

$Z_{24}^* = \{1, 5, 7, 11, 13, 17, 19, 23\}$

$Z_7^* = \{1, 2, 3, 4, 5, 6\}$

Определение

Функция Эйлера $\varphi(m)$— арифметическая функция, значение которой равно количеству натуральных чисел, меньших либо равных m и взаимно простых с ним.

$$\varphi(m) = |Z_m^*|.$$

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

Свойства функции Эйлера

1. p — простое $\Rightarrow \varphi(p) = p - 1$.
2. p — простое $\Rightarrow \varphi(p^k) = p^k - p^{k-1}$.
3. $\gcd(a, b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$.

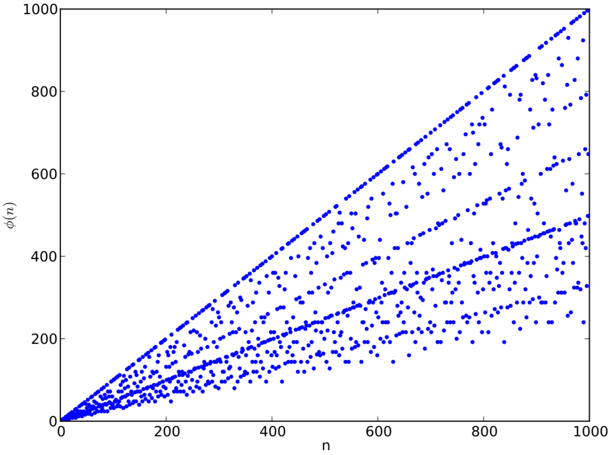
Если $a = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, то

$$\varphi(a) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1}) \ldots (p_s^{k_s} - p_s^{k_s - 1}).$$

$\varphi(21) = \varphi(3)\varphi(7) = 2 \cdot 6 = 12$

$\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = \varphi(2^3)\varphi(3^2)\varphi(5) = (2^3 - 2^2)(3^2 - 3^1)(5 - 1) = 4 \cdot 6 \cdot 4 = 96$

Функция Эйлера



Теорема Эйлера

Теорема (Эйлер)

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

Следствие

Если $\gcd(a, m) = 1$, то
$$a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}.$$

$5^{-1} \pmod{17} \equiv 5^{15} \equiv 5 \cdot 25^7 \equiv 5 \cdot 8^7 \equiv 40 \cdot 64^3 \equiv 6 \cdot (-4)^3 \equiv (-24) \cdot 16 \equiv (-24)(-1) \equiv 24 \equiv 7 \pmod{17}$.

Теорема (Ферма)

Если p — простое, $\gcd(a, p) = 1$, то
$$a^{p-1} \equiv 1 \pmod{p}.$$

Математическая модель симметричной шифрсистемы

Шифрсистемой называется пятерка $\{\mathcal{K}, \mathcal{P}, \mathcal{C}, E, D\}$, где
$\mathcal{K}$ — множество ключей (секретных параметров),
$\mathcal{P}$ — множество открытых текстов,
$\mathcal{C}$ — множество шифртекстов,
E — семейство преобразований зашифрования $E = \{E_k : \mathcal{P} \to \mathcal{C} | k \in \mathcal{K}\}$
D — семейство преобразований расшифрования $D = \{D_k : \mathcal{C} \to \mathcal{P} | k \in \mathcal{K}\}$
с ограничениями

- однозначность расшифрования: $D_k(E_k(p)) = p$ для $\forall p \in \mathcal{P}$;
- реализуемость всех шифртекстов: $\bigcup\limits_{k\in\mathcal{K}} \bigcup\limits_{p\in\mathcal{P}} E_k(p) = \mathcal{C}$, т.е.

  $\forall c \in \mathcal{C} \qquad \exists p \in \mathcal{P}, k \in \mathcal{K}$ такие, что $E_k(p) = c$.

Алфавит

Пусть используется алфавит из m символов. Каждому символу поставим в соответствие число от 0 до $m-1$. Например, английский алфавит «оцифруем» следующим образом:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Классические шифры

- шифры перестановки,
- шифры подстановки,
- композиционные шифры.

Шифр перестановки

- шифрование выполняется блоками, длина блока равна $n > 1$,
- **заменяются не символы открытого текста, а их позиции**,
- секретный параметр шифра — подстановка $\sigma \in S(\{1, 2, 3, \dots, n\})$,
- зашифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $\quad E_\sigma(x) = \sigma(x)$,
- расшифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $D_{(\sigma)}(x) = \sigma^{-1}(x)$,
- однозначность расшифрования:
$$D_\sigma(E_\sigma(x)) = D_\sigma(\sigma(x)) = \sigma^{-1}\sigma(x) = x, \forall x \in A^n$$
- в современной криптографии: P-блок.

$$n = 2,\ \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

VIVATSTUDENT $\to$ VI VA TS TU DE NT $\to$ IV AV ST UT ED TN$\to$ IVAVSTUTEDTN

Шифр перестановки

- шифрование выполняется блоками, длина блока равна $n > 1$,
- **заменяются не символы открытого текста, а их позиции**,
- секретный параметр шифра — подстановка $\sigma \in S(\{1, 2, 3, \ldots, n\})$,
- зашифрование $x = (x_1 x_2 \ldots x_n) \in A^n$: $\quad E_\sigma(x) = \sigma(x)$,
- расшифрование $x = (x_1 x_2 \ldots x_n) \in A^n$: $D_{(\sigma)}(x) = \sigma^{-1}(x)$,
- однозначность расшифрования:

$$D_\sigma(E_\sigma(x)) = D_\sigma(\sigma(x)) = \sigma^{-1}\sigma(x) = x, \forall x \in A^n$$

- в современной криптографии: P-блок.

$$n = 3,\ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

VIVATSTUDENT $\to$ VIV ATS TUD ENT $\to$ IVV TSA UDT NTE$\to$ IVVTSAUDTNTE

Шифр перестановки

- шифрование выполняется блоками, длина блока равна $n > 1$,
- **заменяются не символы открытого текста, а их позиции**,
- секретный параметр шифра — подстановка $\sigma \in S(\{1, 2, 3, \dots, n\})$,
- зашифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $\quad E_\sigma(x) = \sigma(x)$,
- расшифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $D_{(\sigma)}(x) = \sigma^{-1}(x)$,
- однозначность расшифрования:
$$D_\sigma(E_\sigma(x)) = D_\sigma(\sigma(x)) = \sigma^{-1}\sigma(x) = x, \forall x \in A^n$$
- в современной криптографии: P-блок.

Анаграммы

Галилео Галилей	SMAISMRMILMEPOETALEUMIBUNENUGTTAUIRAS
Кеплер	SALVE UMBISTINEUM GEMINATUM MARTIA PROLES (Привет вам, близнецы, Марса порожденье)
Галилео Галилей	ALTISSIMUM PLANETAM TERGEMINUM OBSERVAVI (Высочайшую планету тройною наблюдал)

Классические шифры: шифры подстановки

Шифр подстановки — это метод шифрования, в котором элементы исходного открытого текста заменяются зашифрованным текстом в соответствии с некоторым правилом. Элементами текста могут быть отдельные символы, пары букв, тройки букв, комбинирование этих случаев и так далее.

Получатель сообщения выполняет обратную подстановку для расшифрования

Среди подстановочных шифров выделяют:

- простой замены,
- омофонические,
- полиграммные,
- полиалфавитные.

Шифр сдвига

- определяется пятеркой $\{\mathbb{Z}_m, \mathbb{Z}_m, \mathbb{Z}_m, E, D\}$,
- секретный параметр шифра — величина сдвига $k \in \mathbb{Z}_m$,
- зашифрование $x \in \mathbb{Z}_m$: $\quad E_k(x) = x + k \pmod m$,
- расшифрование $x \in \mathbb{Z}_m$: $D_k(x) = x - k \pmod m$,
- однозначность расшифрования:

$$D_k(E_k(x)) = D_k(x + k \pmod{m}) = x + k - k \pmod{m} = x, \forall x \in \mathbb{Z}_m,$$

- при $k = 3$ — шифр Цезаря,

YLYDW VWXGHQW $\longrightarrow$ VIVAT STUDENT

- в современной криптографии используется в качестве «элементарной» криптографической операции $\ggg$ или $\lll$ для преобразования двоичных n-мерных векторов:

$$x = (x_{n-1}, x_{n-2}, \ldots, x_1, x_0) \xrightarrow{x \ggg k} (x_{k-1}, x_{k-2}, \ldots, x_1, x_0, x_{n-1}, x_{n-2}, \ldots, x_k).$$

Аффинный шифр

- определяется пятеркой $\{\mathbb{Z}_m^* \times \mathbb{Z}_m, \mathbb{Z}_m, \mathbb{Z}_m, E, D\}$,
- секретный параметр шифра $k = (a, b) \in \mathbb{Z}_m^* \times \mathbb{Z}_m$,
- зашифрование $x \in \mathbb{Z}_m$: $E_{(a,b)}(x) = ax + b \pmod{m}$,
- расшифрование $x \in \mathbb{Z}_m$: $D_{(a,b)}(x) = a^{-1}(x - b) \pmod{m}$,
- однозначность расшифрования:

$$D_k(E_k(x)) = D_k(ax+b \pmod{m}) = a^{-1}(ax+b-b) \pmod{m} = x, \forall x \in \mathbb{Z}_m$$

- при $a = 1$ — шифр сдвига,

Пусть $\mathcal{A} = \{A, B, C, D, E\}$, зашифруем аффинным шифром сообщение «DA» на ключе $(2, 3)$:

D$\to 3$ $E_{(2,3)}(3) = 2 \cdot 3 + 3 \pmod{5} = 4 \to$ E

A$\to 0$ $E_{(2,3)}(0) = 2 \cdot 0 + 3 \pmod{5} = 3 \to$ D

DA $\longrightarrow$ ED

$\{\mathbb{Z}_{26}^* \times \mathbb{Z}_{26}, \mathbb{Z}_{26}, \mathbb{Z}_{26}, E, D\}$ ключ $(2, 3) \notin \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$:

$$E_{(2,3)}(0) = 2 \cdot 0 + 3 \pmod{26} = 3,$$
$$E_{(2,3)}(13) = 2 \cdot 13 + 3 \pmod{26} = 3$$

Шифр простой замены

- определяется пятеркой $\{S(\mathbb{Z}_m), \mathbb{Z}_m, \mathbb{Z}_m, E, D\}$,
- секретный параметр шифра — подстановка $\sigma \in S(\mathbb{Z}_m)$,
- зашифрование $x \in \mathbb{Z}_m$: $\quad E_\sigma(x) = \sigma(x)$,
- расшифрование $x \in \mathbb{Z}_m$: $D_{(\sigma)}(x) = \sigma^{-1}(x)$,
- однозначность расшифрования:

$$D_\sigma(E_\sigma(x)) = D_\sigma(\sigma(x)) = \sigma^{-1}\sigma(x) = x, \forall x \in \mathbb{Z}_m,$$

- в современной криптографии: S-блок.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 \\ 16 & 22 & 4 & 17 & 19 & 24 & 20 & 8 & 14 & 15 & 0 & 18 & 3 & 5 & 6 & 7 & 9 & 10 & 11 & 25 & 23 & 2 & 21 & 1 & 13 & 12 \end{pmatrix}$$

VIVAT STUDENT $\longrightarrow$ COCQZ LZXRTFZ

Шифр подстановки vs шифр перестановки

Пусть $\mathcal{A} = \{A, B, C, D\}$

Шифр подстановки

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$

AAAA $\to$ CCCC

CCCD $\to$ AAAB

Шифр перестановки

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$

AAAA $\to$ AAAA

CCCD $\to$ CDCC

Шифр омофонической замены

Один из способов защиты от частотной криптоатаки. Каждая буква текста шифруется несколькими символами этого или другого алфавита. Число этих символов пропорционально частотной характеристике шифруемой буквы. Например:

Буква	Омофоническая замена							
A	17	19	34	41	56	60	67	83	
I	08	22	53	65	88	90			
L	03	44	76						
N	02	09	15	27	32	40	59		
O	01	11	23	42	54	70	80		
P	33	91							
T	05	10	20	29	45	58	64	78	99

PLAIN PILOT $\longrightarrow$ 91 44 56 65 59 33 08 76 28 78

Шифр Виженера

- определяется пятеркой $\{A^*, A^*, A^*, E, D\}$, где $A = \mathbb{Z}_m$,
- секретный параметр шифра — ключевое слово длины n, определяющее n шифров сдвига : $k = (k_0, \dots, k_{n-1})$,
- зашифрование $x = (x_1 x_2 \dots) \in A^*$:

$$E_k(x_i) = x_i + k_{i \bmod n} \pmod{m}, \qquad i = 1, 2, \dots,$$

- расшифрование $x = (x_1 x_2 \dots) \in A^*$:

$$D_k(x_i) = x_i - k_{i \bmod n} \pmod{m}, \qquad i = 1, 2, \dots,$$

- однозначность расшифрования следует из однозначности расшифрования для шифра сдвига
- в современной криптографии: построение поточных алгоритмов шифрования на основе наложения гаммы на открытый текст.

								$\to$							
открытый текст:	S	T	U	D	E	N	T	$\to$	18	19	20	3	4	13	19
ключевое слово:	E	D	U	E	D	U	E	$\to$	4	3	20	4	3	20	4
шифртекст:	W	W	O	H	H	H	X	$\to$	22	22	14	7	7	7	23

Шифр Хилла

- шифрование выполняется блоками, длина блока равна $n > 1$, алфавит $A = \mathbb{Z}_m$,
- секретный параметр шифра — обратимая матрица M размера $n \times n$ над $\mathbb{Z}_m$, при этом $\det M \in \mathbb{Z}_m^*$;
- зашифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $\quad E_M(x) = xM$,
- расшифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $D_{(M)}(x) = xM^{-1}$,
- в современной криптографии: MDS матрицы.

Шифр Хилла

- шифрование выполняется блоками, длина блока равна $n > 1$, алфавит $A = \mathbb{Z}_m$,
- секретный параметр шифра — обратимая матрица M размера $n \times n$ над $\mathbb{Z}_m$, при этом $\det M \in \mathbb{Z}_m^*$;
- зашифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $\quad E_M(x) = xM$,
- расшифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $D_{(M)}(x) = xM^{-1}$,
- в современной криптографии: MDS матрицы.

$$n = 2,\ A = \mathbb{Z}_m,$$

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \in \mathbb{Z}_m^{2\times 2}$$

$$\det M = m_{11}m_{22} - m_{12}m_{21} \in \mathbb{Z}_m^*.$$

$$M^{-1} = (\det M)^{-1} \begin{pmatrix} m_{22} & -m_{12} \\ -m_{21} & m_{11} \end{pmatrix} \pmod m$$

Шифр Хилла

- шифрование выполняется блоками, длина блока равна $n > 1$, алфавит $A = \mathbb{Z}_m$,
- секретный параметр шифра — обратимая матрица M размера $n \times n$ над $\mathbb{Z}_m$, при этом $\det M \in \mathbb{Z}_m^*$;
- зашифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $\quad E_M(x) = xM$,
- расшифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $D_{(M)}(x) = xM^{-1}$,
- в современной криптографии: MDS матрицы.

$$n = 2,\ A = \{\text{A,B,C,D,E}\} \to \mathbb{Z}_5 = \{0, 1, 2, 3, 4\},$$

$$M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Шифр Хилла

- шифрование выполняется блоками, длина блока равна $n > 1$, алфавит $A = \mathbb{Z}_m$,
- секретный параметр шифра — обратимая матрица M размера $n \times n$ над $\mathbb{Z}_m$, при этом $\det M \in \mathbb{Z}_m^*$;
- зашифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $\quad E_M(x) = xM$,
- расшифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $D_{(M)}(x) = xM^{-1}$,
- в современной криптографии: MDS матрицы.

$$n = 2,\ A = \{\mathrm{A,B,C,D,E}\} \to \mathbb{Z}_5 = \{0, 1, 2, 3, 4\},$$

$$M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

$$\det M = 1 \cdot 4 - 2 \cdot 3 \equiv 3 \pmod 5 \neq 0, \qquad \gcd(3, 5) = 1,$$
$$(\det M)^{-1} = (3)^{-1} \pmod 5 \equiv 2 \pmod 5,$$
$$M^{-1} = 2 \cdot \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} \pmod 5 = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$$

Шифр Хилла

- шифрование выполняется блоками, длина блока равна $n > 1$, алфавит $A = \mathbb{Z}_m$,
- секретный параметр шифра — обратимая матрица M размера $n \times n$ над $\mathbb{Z}_m$, при этом $\det M \in \mathbb{Z}_m^*$;
- зашифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $\quad E_M(x) = xM$,
- расшифрование $x = (x_1 x_2 \dots x_n) \in A^n$: $D_{(M)}(x) = xM^{-1}$,
- в современной криптографии: MDS матрицы.

$$'\mathrm{CD}' \to (2,3) = x : \qquad E_M(x) = (2,3)\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = (1,1) \to '\mathrm{BB}'$$

$$'\mathrm{BB}' \to (1,1) = x : \qquad D_M(x) = (1,1)\begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix} = (2,3) \to '\mathrm{CD}'$$