Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

Историческая криптография

История развития криптографии

Краткая история

XL в. до н.э. — XIX в. н.э.: элементарная (наивная) криптография, моноалфавитные и полиалфавитные шифры.

XIX в. — начало XX в.: появление математической криптографии, формирование требований к надежным шифрам, создание шифровальных машин.

1930-е гг. — 1970-е гг.: формирование современной криптографии с секретным ключом.

1970-е гг. — 1990-е гг.: формирование всех направлений современной криптографии, появление идей квантовой и постквантовой криптографии.

Наше время: разработки в области квантовой и постквантовой криптографии.

Подстановочные шифры

Подстановочные шифры

- Криптографическое преобразование заключается в **замене символов** открытого текста на другие символы по определенному правилу:
  - символы шифртекста принадлежат тому же алфавиту естественного языка, что и символы открытого текста;
  - символы шифртекста записываются как числа или графические образы.
- **Примеры шифров:**
  - Атбаш
  - Линейка Энея
  - Квадрат Полибия
  - Шифр простой замены
  - Шифр Цезаря
  - Аффинный шифр
  - Диск Альберти
  - …

Шифр простой замены

- Открытый текст: $x = (x_1, \ \ldots, \ x_l)$, где $x_i \in A = \{a_1, a_2, \ldots, a_m\}$;
- Шифртекст: $y = (y_1, \ \ldots, \ y_l)$, где $y_i \in A = \{a_1, a_2, \ldots, a_m\}$;
- Ключ: $k = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \\ a_{i_1} & a_{i_2} & \cdots & a_{i_m} \end{pmatrix}$;
- Зашифрование: $E_k(x) = E_k(x_1, \ \ldots, \ x_l) = \big(k(x_1), \ \ldots, \ k(x_l)\big)$;
- Расшифрование: $D_k(y) = D_k(y_1, \ \ldots, \ y_l) = \big(k^{-1}(y_1), \ \ldots, \ k^{-1}(y_l)\big)$.

Аффинный шифр

- Открытый текст: $x = (x_1, \ \ldots, \ x_l)$, где $x_i \in \mathbb{Z}_m$;
- Шифртекст: $y = (y_1, \ \ldots, \ y_l)$, где $y_i \in \mathbb{Z}_m$;
- Ключ: $k = (\alpha, \beta)$, $\alpha \in \mathbb{Z}_m^*$, $\beta \in \mathbb{Z}_m$;
- Зашифрование: $E_k(x_i) = y_i = \alpha x_i + \beta$;
- Расшифрование: $D_k(y_i) = x_i = (y_i - \beta)\alpha^{-1}$.

Аффинный рекуррентный шифр

- Открытый текст: $x = (x_1, \ \ldots, \ x_l)$, где $x_i \in \mathbb{Z}_m$;
- Шифртекст: $y = (y_1, \ \ldots, \ y_l)$, где $y_i \in \mathbb{Z}_m$;
- Ключ: $k_1 = (\alpha_1, \beta_1), k_1 \in \mathbb{Z}_m^* \times \mathbb{Z}_m$;

  $k_2 = (\alpha_2, \beta_2), k_2 \in \mathbb{Z}_m^* \times \mathbb{Z}_m$;

  $k_i = (\alpha_i, \beta_i) = (\alpha_{i-1}\alpha_{i-2}, \ \beta_{i-1} + \beta_{i-2}), i = \overline{3, l}$;
- Зашифрование: $E_k(x_i) = y_i = \alpha_i x_i + \beta_i$;
- Расшифрование: $D_k(y_i) = x_i = (y_i - \beta_i)\alpha_i^{-1}$.

Примеры шифрования

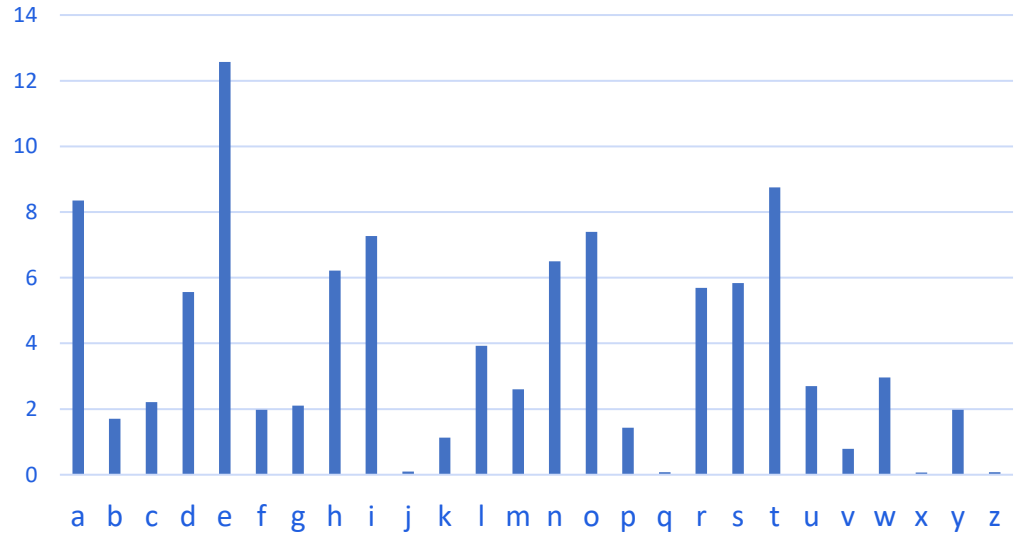
- Сообщение:
  - $X = CRYPTOGRAPHY$
- Ключ шифра простой замены:
  - $k = \begin{pmatrix} A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & P & Q & R & S & T & U & V & W & X & Y & Z \\ E & K & H & M & G & C & P & T & L & R & A & Q & F & X & W & N & Y & I & Z & B & V & U & O & S & D & J \end{pmatrix}$
- Ключ аффинного шифра:
  - $k = (3{,}10)$
- Ключ аффинного рекуррентного шифра:
  - $k_1 = (3,\ 10); k_2 = (5,\ 4)$

Примеры шифрования

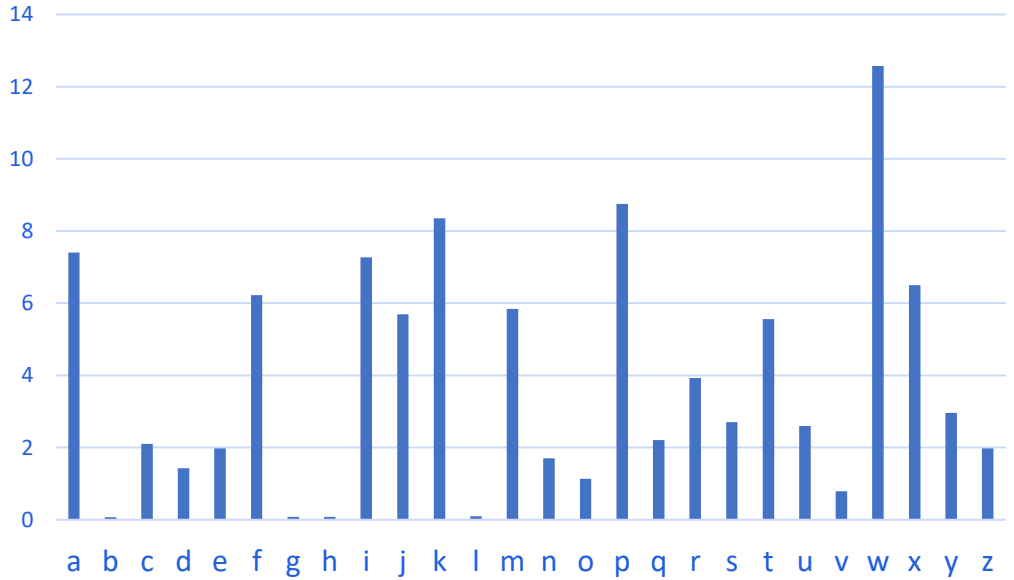
- Шифртекст, полученный по шифру простой замены:
  - $Y = HIDNBWPIENTD$
- Шифртекст, полученный по аффинному шифру:
  - $Y = QJEDPACJKDFE$
- Шифртекст, полученный по аффинному рекуррентному шифру:
  - $Y = QLKZJQGNGTNS$

Частотный криптоанализ шифров простой замены

Частота встречаемости символов английского языка, %



Частота встречаемости символов шифртекста, %



Перестановочные шифры

Перестановочные шифры

- Криптографическое преобразование заключается в **перестановке местами символов** открытого текста по определенному правилу.

- **Примеры шифров:**
  - Сцитала
  - Шифр на основе поворотной решетки
  - Блочный перестановочный шифр
  - …

Шифр на основе поворотной решетки

- Поворотная решетка представляет собой квадратный лист из твердого материала (картона, металла и т.п.), который содержит несколько квадратных прорезей-окон.
- Решетка накладывается на лист бумаги и в окна вписываются символы сообщения.
- После заполнения всех окон решетка поворачивается на 90 градусов, в результате чего окна накладываются на новые чистые участки листа бумаги и в них вписываются следующие символы сообщения.
- Если выбранная решетка не обеспечивает полного заполнения листа, либо сообщение имеет размер меньше максимально возможного, то на оставшиеся пустые места записываются случайные символы.

Пример шифрования

Исходное положение

	C		R
	Y		

Первый поворот

	C		R
	Y	P	T
			O

Второй поворот

	C		R
	Y	P	T
		G	
R		A	O

Третий поворот

P	C		R
	Y	P	T
H	Y	G	
R		A	O

Случайное заполнение

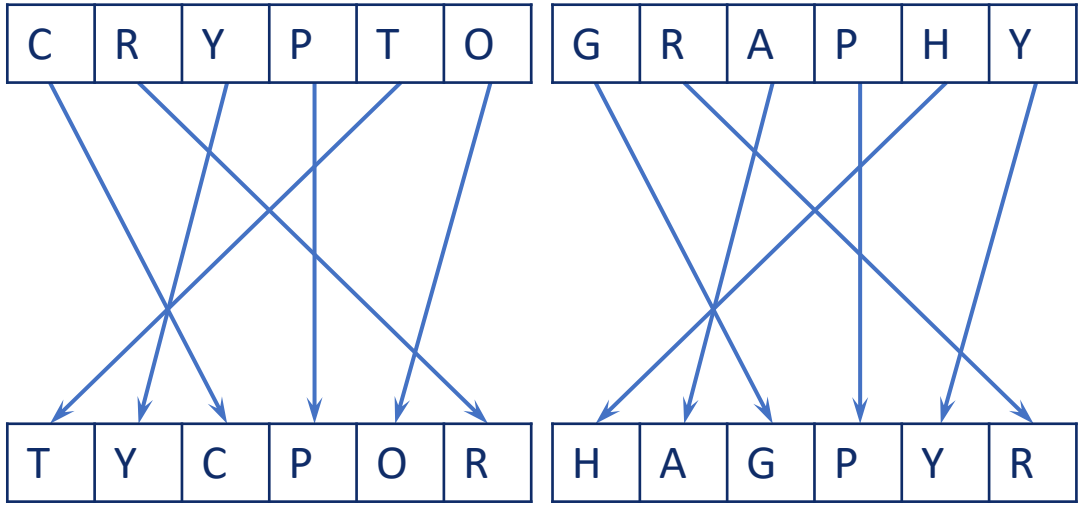
P	C	D	R
F	Y	P	T
H	Y	G	S
R	A	A	O

Блочный перестановочный шифр

- Блок открытого текста: $x = (x_1, \ \dots, \ x_l)$, где $x_i \in A = \{a_1, a_2, \dots, a_m\}$;
- Блок шифртекста: $y = (y_1, \ \dots, \ y_l)$, где $y_i \in A = \{a_1, a_2, \dots, a_m\}$;
- Ключ: $k = \begin{pmatrix} 1 & \cdots & l \\ i_1 & \cdots & i_l \end{pmatrix}$;
- Зашифрование: $E_k(x) = \left(x_{k(1)}, \ \dots, \ x_{k(l)}\right)$;
- Расшифрование: $E_k(y) = \left(y_{k^{-1}(1)}, \ \dots, \ y_{k^{-1}(l)}\right)$.

Пример шифрования

- Сообщение:
  - $X = CRYPTOGRAPHY$
- Ключ блочного перестановочного шифра:
  - $k = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 4 & 6 & 2 \end{pmatrix}$
- Шифртекст:
  - $Y = TYCPORHAGPYR$



Блочные шифры

Блочные шифры

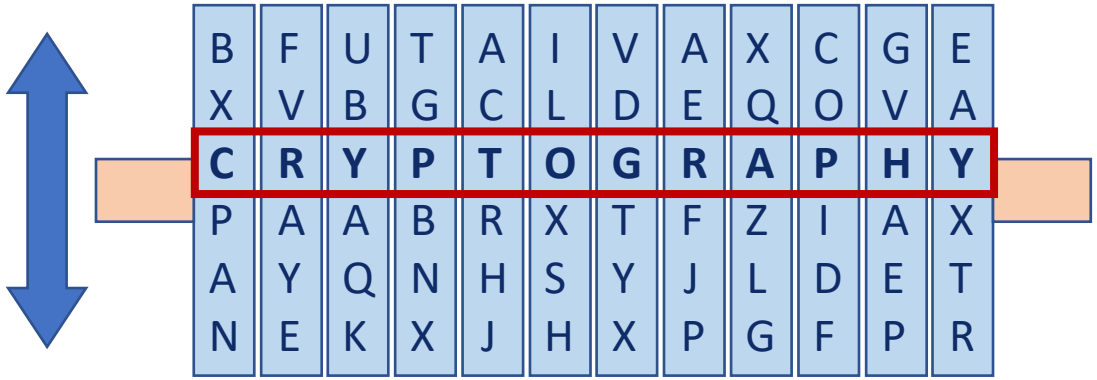
- Открытый текст **разбивается на блоки равной длины**, одно и то же криптографическое преобразование применяется к каждому блоку.
- Блочный шифр можно рассматривать как шифр замены над множеством всевозможных состояний блока символов открытого текста.

- **Примеры шифров:**
  - Шифр Порта
  - Шифр Плейфера
  - Блочный перестановочный шифр
  - Дисковый шифратор Джефферсона
  - Шифр Хилла
  - Аффинный блочный шифр
  - …

Дисковый шифратор Джефферсона

- Шифровальное устройство представляет собой цилиндр, состоящий из 36 дисков, насаженных на общую ось, вокруг которой их можно вращать. На боковой поверхности каждого диска выписан английский алфавит в некотором порядке.
- Для зашифрования блока сообщения выбирается линия, параллельная оси. Диски поворачиваются так, чтобы символы на выбранной линии образовали блок сообщения. В качестве блока шифртекста берется последовательность символов, находящихся на любой другой линии.

Шифратор из 12 дисков



Шифр Хилла

- Блок открытого текста: $X = (x_1 \ \dots \ x_n)^{\mathrm{T}}$, где $x_i \in \mathbb{Z}_m$;
- Блок шифртекста: $Y = (y_1 \ \dots \ y_n)^{\mathrm{T}}$, где $y_i \in \mathbb{Z}_m$;
- Ключ: матрица $K = \left(k_{i,j}\right)_{i=1,j=1}^{n,n}$, $k_{i,j} \in \mathbb{Z}_m$, $|K| \in \mathbb{Z}_m^*$;
- Зашифрование: $E_K(X) = K \cdot \mathrm{X} = \mathrm{Y}$;
- Расшифрование: $D_K(Y) = K^{-1} \cdot Y = X$.

Рекуррентный шифр Хилла

- Блок открытого текста: $X = (x_1 \ \dots \ x_n)^{\mathrm{T}}$, где $x_i \in \mathbb{Z}_m$;
- Блок шифртекста: $Y = (y_1 \ \dots \ y_n)^{\mathrm{T}}$, где $y_i \in \mathbb{Z}_m$;
- Ключ: матрица $K_1 = \left(k_{i,j}\right)_{i=1,j=1}^{n,n}$, $k_{i,j} \in \mathbb{Z}_m$, $|K_1| \in \mathbb{Z}_m^*$;

  матрица $K_2 = \left(k_{i,j}\right)_{i=1,j=1}^{n,n}$, $k_{i,j} \in \mathbb{Z}_m$, $|K_2| \in \mathbb{Z}_m^*$;

  $K_i = K_{i-2} \cdot K_{i-1}$, $i = \overline{3, l}$;
- Зашифрование: $E_{K_i}(X_i) = K_i \cdot X_i = Y_i$;
- Расшифрование: $D_{K_i}(Y_i) = K_i^{-1} \cdot Y_i = X_i$.

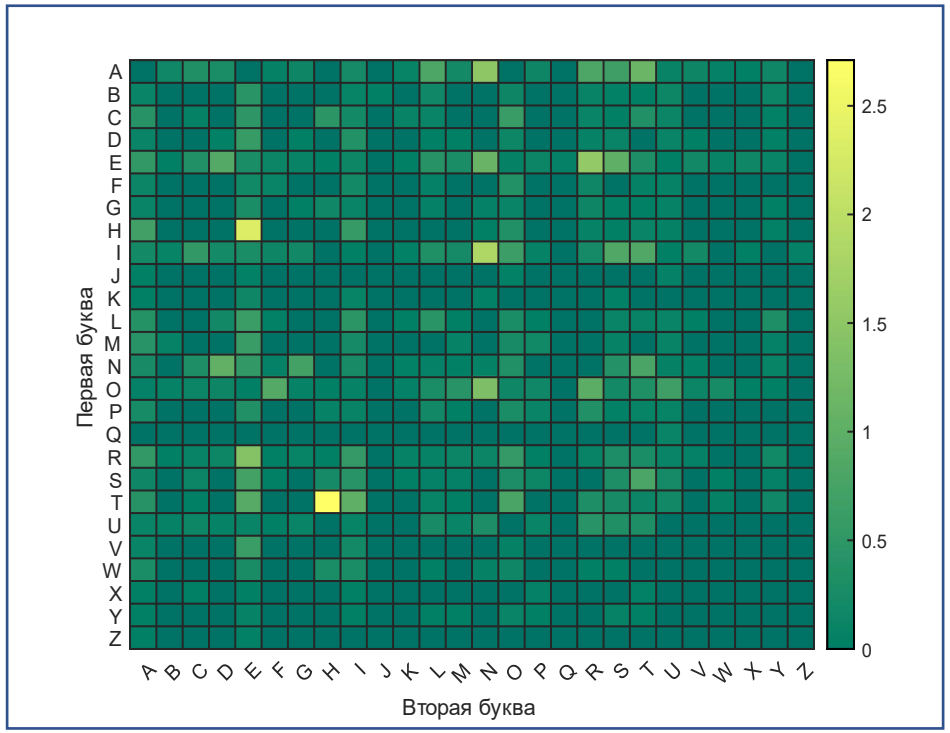
Примеры шифрования

- Сообщение:
  - $X = CRYPTOGRAPHY,$
  - $X_1 = \begin{bmatrix} 2 \\ 17 \\ 24 \\ 15 \end{bmatrix}, X_2 = \begin{bmatrix} 19 \\ 14 \\ 6 \\ 17 \end{bmatrix}, X_3 = \begin{bmatrix} 0 \\ 15 \\ 7 \\ 24 \end{bmatrix}.$
- Ключ:
  - $K = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 5 & 0 & 2 & 3 \\ 2 & 1 & 1 & 7 \\ 3 & 4 & 1 & 4 \end{bmatrix}, |K| = 19 \in \mathbb{Z}_{26}^{*}.$
- Зашифрование:
  - $Y_1 = K \cdot X_1 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 5 & 0 & 2 & 3 \\ 2 & 1 & 1 & 7 \\ 3 & 4 & 1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 17 \\ 24 \\ 15 \end{bmatrix} = \begin{bmatrix} 18 \\ 25 \\ 20 \\ 2 \end{bmatrix},$
  - $Y_2 = K \cdot X_2 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 5 & 0 & 2 & 3 \\ 2 & 1 & 1 & 7 \\ 3 & 4 & 1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 14 \\ 6 \\ 17 \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \\ 21 \\ 5 \end{bmatrix},$
  - $Y_3 = K \cdot X_3 = \begin{bmatrix} 1 & 3 & 5 & 7 \\ 5 & 0 & 2 & 3 \\ 2 & 1 & 1 & 7 \\ 3 & 4 & 1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 15 \\ 7 \\ 24 \end{bmatrix} = \begin{bmatrix} 14 \\ 8 \\ 8 \\ 7 \end{bmatrix},$
  - $Y = SZUCCCVFOIIH.$

Криптоанализ блочных шифров

- Частотный криптоанализ:
  - Блочные шифры устойчивы к простому частотному криптоанализу на основе подсчета частоты встречаемости отдельных символов;
  - Блочные шифры уязвимы перед n-граммным (поблочным) частотным криптоанализом.
- Криптоанализ на основе открытых текстов.

Частота встречаемости биграмм в английском языке



Шифры гаммирования

Шифры гаммирования

- Криптографическое преобразование заключается в наложении на открытый текст последовательности символов той же длины (**гаммы**), генерируемой на основе ключа шифрования.
- Под наложением гаммы понимается операция, которая каждой паре (**символ открытого текста, символ гаммы**) ставит в соответствие **символ шифртекста** по определенному правилу.

- **Примеры шифров:**
  - Шифр табличного гаммирования
  - Шифр Виженера
  - Шифр Вернама
  - …

Табличное гаммирование

- Формируется латинский квадрат – квадратная таблица $m \times m$, каждая строка и каждый столбец которой представляют собой некоторую перестановку алфавита A. Строки и столбцы данной таблицы помечаются символами алфавита в естественном порядке. Латинский квадрат может быть как секретным, так и открытым.
- Для открытого текста $x = (x_1, \ldots, x_l)$, записанного в символах некоторого алфавита A, $|A| = m$, из символов того же алфавита формируется **гамма** – последовательность символов $\gamma = (\gamma_1, \ldots, \gamma_l)$ той же длины, что и открытый текст.
- Зашифрование состоит в наложении гаммы на открытый текст, когда каждой паре (x_i, γ_i) с помощью латинского квадрата ставится в соответствие символ шифртекста y_i.

Табличное гаммирование

- Зашифрование:
  - выбирается строка латинского квадрата, соответствующая символу x_i;
  - выбирается столбец латинского квадрата, соответствующий символу γ_i;
  - в качестве символа шифртекста y_i принимается символ, находящийся в таблице на пересечении выбранных строки и столбца.
- Расшифрование:
  - выбирается столбец латинского квадрата, соответствующий символу γ_i;
  - в выбранном столбце находится символ со значением y_i;
  - в качестве символа открытого текста x_i принимается символ, которым помечена соответствующая строка латинского квадрата.

Пример шифрования

- Алфавит: $A = \{a, b, c, d, e\}$
- Открытый текст: $x = dbcbcded$
- Гамма: $\gamma = abcabcab$
- Латинский квадрат:

$\circ$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$	$\boldsymbol{e}$
$\boldsymbol{a}$	b	d	a	e	c
$\boldsymbol{b}$	d	a	c	b	e
$\boldsymbol{c}$	e	c	b	a	d
$\boldsymbol{d}$	a	e	d	c	b
$\boldsymbol{e}$	c	b	e	d	a

- Зашифрование:
  - $y_1 = x_1 \circ \gamma_1 = d \circ a = a;$
  - $y_2 = x_2 \circ \gamma_2 = b \circ b = a;$
  - $y_3 = x_3 \circ \gamma_3 = c \circ c = b;$
  - $y_4 = x_4 \circ \gamma_4 = b \circ a = d;$
  - $y_5 = x_5 \circ \gamma_5 = c \circ b = c;$
  - $y_6 = x_6 \circ \gamma_6 = d \circ c = d;$
  - $y_7 = x_7 \circ \gamma_7 = e \circ a = c;$
  - $y_8 = x_8 \circ \gamma_8 = d \circ b = e.$

Шифр Виженера

- Открытый текст: $x = (x_1, \ \ldots, \ x_l)$, где $x_i \in \mathbb{Z}_m$;
- Шифртекст: $y = (y_1, \ \ldots, \ y_l)$, где $y_i \in \mathbb{Z}_m$;
- Ключ: $k = (k_1, \ \ldots, \ k_r)$, где $k_i \in \mathbb{Z}_m, r < l$;
- Гамма: $\gamma = (\gamma_1, \ \ldots, \ \gamma_l)$, где $\gamma_i \in \mathbb{Z}_m$;
- Зашифрование: $E_k(x_i) = y_i = (x_i + \gamma_i) \bmod m$;
- Расшифрование: $D_k(y_i) = x_i = (y_i - \gamma_i) \bmod m$.

Способы выработки гаммы

- Повторение ключа: $\gamma = (k_1,\ \ldots,\ k_r, k_1,\ \ldots,\ k_r, k_1,\ \ldots,\ k_r, \ldots);$
- Самоключ по открытому тексту: $\gamma = (k_1,\ x_1,\ \ldots,\ x_{l-1});$
- Самоключ по шифртексту: $\gamma = (k_1,\ y_1,\ \ldots,\ y_{l-1}).$

Примеры шифрования

- Повторение ключа:
  - Сообщение: $x = CRYPTOGRAPHY = (2, 17, 24, 15, 19, 14, 6, 17, 0, 15, 7, 24).$
  - Ключ: $k = KEY = (10, 4, 24).$
  - Гамма: $\gamma = KEYKEYKEYKEY = (10, 4, 24, 10, 4, 24, 10, 4, 24, 10, 4, 24).$
  - Шифртекст: $y = MVWZXMQVYZLW = (12, 21, 22, 25, 23, 12, 16, 21, 24, 25, 11, 22).$

Примеры шифрования

- Самоключ по открытому тексту:
  - Сообщение: $x = CRYPTOGRAPHY = (2, 17, 24, 15, 19, 14, 6, 17, 0, 15, 7, 24).$
  - Ключ: $k = K = (10).$
  - Гамма: $\gamma = KCRYPTOGRAPH = (10, 2, 17, 24, 15, 19, 14, 6, 17, 0, 15, 7).$
  - Шифртекст: $y = MTPNIHUXRPWF = (12, 19, 15, 13, 8, 20, 23, 17, 15, 22, 5).$

Примеры шифрования

- Самоключ по шифртексту:
  - Сообщение: $x = CRYPTOGRAPHY = (2, 17, 24, 15, 19, 14, 6, 17, 0, 15, 7, 24).$
  - Ключ: $k = K = (10).$
  - Гамма: $\gamma = KMDBQJXDUUJQ = (10, 12, 3, 1, 16, 9, 23, 3, 20, 20, 9, 16).$
  - Шифртекст: $y = MDBQJXDUUJQO = (12, 3, 1, 16, 9, 23, 3, 20, 20, 9, 16, 14).$

Шифр Вернама

- Открытый текст: $x = (x_1, \ \ldots, \ x_l)$, где $x_i \in \mathbb{Z}_2$;
- Шифртекст: $y = (y_1, \ \ldots, \ y_l)$, где $y_i \in \mathbb{Z}_2$;
- Гамма: $\gamma = (\gamma_1, \ \ldots, \ \gamma_l)$, где $\gamma_i \in \mathbb{Z}_2$;
- Зашифрование: $E_k(x_i) = y_i = (x_i + \gamma_i) \bmod 2$;
- Расшифрование: $D_k(y_i) = x_i = (y_i - \gamma_i) \bmod 2$.

- **Ключевое требование** – каждая гамма вырабатывается случайным образом и используется только один раз.

Криптоанализ шифров гаммирования

- Шифр Виженера с повторяющимся ключам уязвим перед двухэтапным статистическим криптоанализом:
  - вычисление длины ключа с помощью теста Касиски или индекса совпадений;
  - вычисление символов ключа посредством частотного анализа.
- Восстановление открытых текстов зашифрованных с использованием общей гаммы.

Спасибо за внимание!

Евсютин Олег Олегович
Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21
oevsyutin@hse.ru