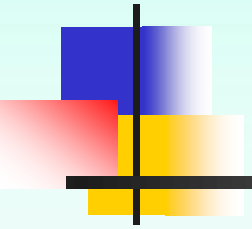
CRYPTOGRAPHY



МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Лек. 6 2022 КІБ-19

КРИПТОАНАЛИЗ. АТАКИ

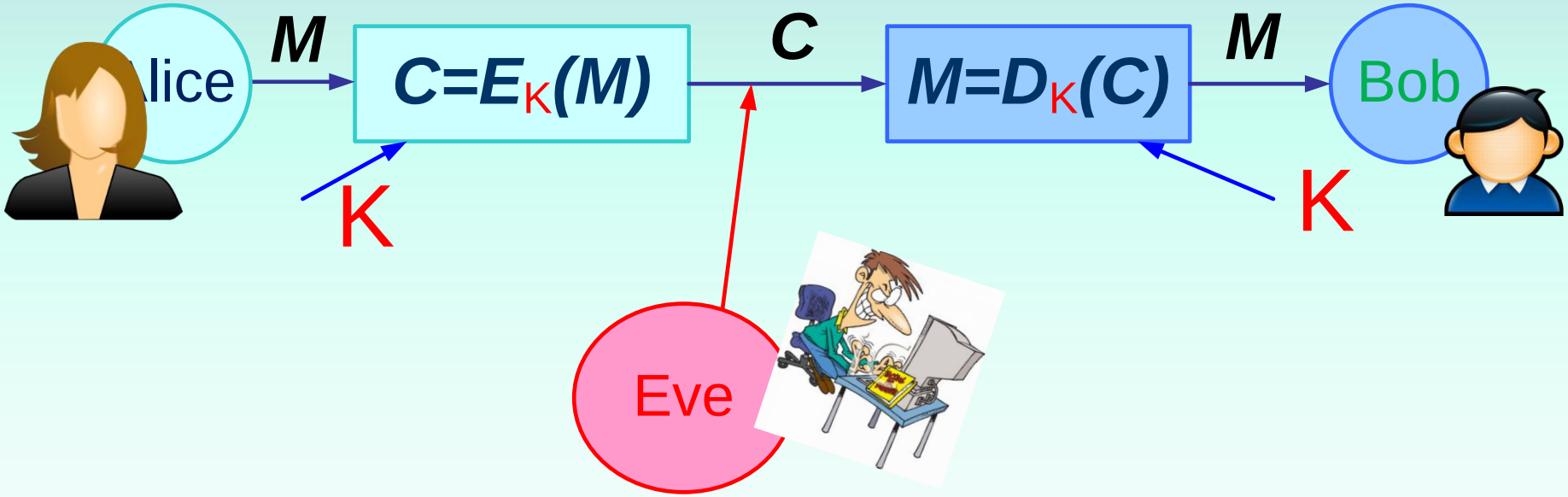
Криптоанализ

Наука Криптоанализ от др. греческого κρυπτός «скрытый» + «анализ» — наука о методах **дешифровки** зашифрованной информации без предназначенного для этого ключа, а также сам процесс такой дешифровки.

Криптоанализ включает также методы выявления уязвимости криптографических алгоритмов или протоколов.

Попытка раскрытия шифра с применением методов криптоанализа → **криптографическая атака** на этот шифр

Алгоритм шифрования



Атаки

- **Атака** с использованием только шифрованного текста ***C → ? K, M*** .
- **Атака** с известным открытым текстом ***C,M → ?K .***
- **Атака** с избранным открытым текстом.
- **Атака** с избранным шифрованным текстом.
- **Атака** на базе парадокса задачи о днях рождения.
- **Двухсторонние атака** («встреча на середине»).
- **Атака** со связанным ключом.
- **Атака** с избранным ключом.
- Дифференциальный крито анализ.

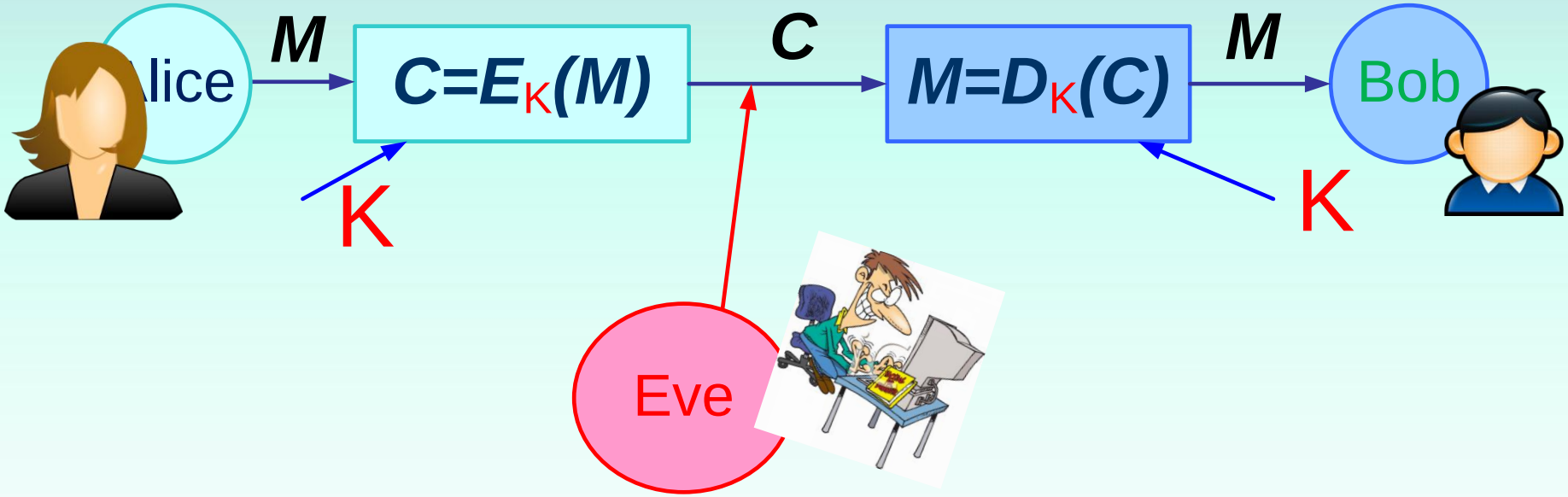
Методы атак

- **Полный перебор (**«грубой силы», brute force attack**)** - перебор ключей. Оценивается мощностью множества ключей $\|K\|$.
- **Статистический анализ –** учет статистики появления символов в «разумном» тексте.

- **XSL атака –** основан на алгебраических свойствах шифра. Решение особой системы уравнений.
- **Сдвиговая атака** - блочные шифры, циклическое повторение ключей.
- **Дифференциальные методы.**
- **Метод бумеранга.**

ШИФРЫ ПОДСТАНОВОК И ПЕРЕСТАНОВОК

Алгоритм шифрования



ОДИН КЛЮЧ

как для шифрования, так и дешифрования

$$!!!\ D_K(*) = E_K^{-1}(*)$$

$$M = D_K(E_K(M))$$

Симметричные шифры

K2 = K1= K

СИММЕТРИЧНЫЕ (ОДНОКЛЮЧЕВЫЕ)

- **I. ЗАМЕНЫ /ПОДСТАНОВКИ**
- ПЕРЕСТАНОВКИ
- ГАММИРОВАНИЕ
- КВАНТОВЫЕ

Шифры подстановок

Идея → замена одного символа другим .

I.2. иногда «ПОЛИАЛФАВИТНЫЕ»

I.2. Многоалфавитные шифры

Идея → символ в открытом тексте заменяется на некоторый другой символ в шифротексте. **НО!** Символ замены (символ в шифротексте) **зависит** от позиции символа в открытом тексте. Отношение → **один ко многим!**

$$M = \{s | s \in \mathbb{Z}_n\}, C = \{c | c \in \mathbb{Z}_n\}, K = \{k | k \in \mathbb{Z}_n\}$$

$mss = s_0, s_1, \ldots, s_t, \ldots \quad s_t \in M;$

$ctxt = c_0, c_1, \ldots, c_t, \ldots \quad c_t \in C;$

Здесь t – номер символа в последовательности.

Формируется → $key = k_0, k_1, \ldots, k_t, \ldots;$

$$k_t = F\left(t, s_t, k_{j=f(s)}\right),$$

$$c_t = (s_t + k_t) \bmod n; \; s_t = (c_t - k_t) \bmod n$$

I.2.1 Автоключевой шифр

Идея →

Задается секретный k_0 ! $c_0 = s_0$

$$k_t = s_{t-1}, \qquad t = 1,2, \ldots$$

Шифрование → $c_t = (s_t + k_t) \bmod n$

Дешифрование → $s_t = (c_t - k_t) \bmod n$

мощность $\|K\| = n$

Ограничиваемся БОЛЬШИМИ

А Б В Г Д Е Є Ж З И І Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ю Я _

Задаем секретный k_0 ! $k_{t+1} = s_t, t = 0,1,2, \ldots$

Шифрование → $c_t = (s_t + k_t)(mod 31)$

Дешифрование → $s_t = (c_t - k_t)\,(mod 31)$

I.2.2 Шифр Виженера (Vigenere, 1585)

Идея→ задается вектор $\boldsymbol{K}$ ключей $(\boldsymbol{m < n})$ – секретное кодовое слово

$$\boldsymbol{K} = \begin{bmatrix} \boldsymbol{k}_0 \\ \boldsymbol{k}_i \\ \boldsymbol{k}_{m-1} \end{bmatrix} \qquad \boldsymbol{k}_i = \boldsymbol{s}_l \in \mathbb{Z}_{\boldsymbol{n}}!$$

Шифрование → $\boldsymbol{c_t = \left(s_t + k_{t(mod\, m)}\right) mod\, n}$

Дешифрование → $\boldsymbol{s_i = \left(c_t - k_{t(mod\, m)}\right) mod\, n}$

I.2.2 Шифр Виженера. Пример

К = СУПЕРКЛЮЧ

М= ПРИВІТ_СТУДЕНТИ_КІБ

М= *ПРИВІТ_СТ УДЕНТИ_КІ Б*

k_0 = С → 20; s_0 = П → 18;

c_0 = (20+18) mod 31 = 7; c_0 = 7 → Є

С = ЄИЩЗЯШЛПН ІШХУЗНЛІЕ У

I.2.3 Шифр Плейфера // Playfair (Wheatstone, 1854)

Идея→ задается $\boldsymbol{m * m}$ матрица $\boldsymbol{K}$ ключей $(\boldsymbol{m * m \geq n})$

$$\begin{bmatrix} \boldsymbol{k_{0,0}} & \boldsymbol{\dots} & \boldsymbol{k_{0,m}} \\ & \boldsymbol{k_{i,j}} & \\ \boldsymbol{k_{m,0}} & & \boldsymbol{k_{m,m}} \end{bmatrix} \qquad \boldsymbol{k_{i,j} = s_l \in \mathbb{Z}_n!}$$

Каждый $\boldsymbol{k_{i,j}}$ есть символ алфавита.

Размещение $\boldsymbol{k_{i,j}}$ в матрице $\boldsymbol{K}$ собственно и есть секретный ключ.

Мощность $\boldsymbol{\|K\| = (m * m)!}$

Открытый текст $\boldsymbol{s_0, s_1, s_2, s_3, \dots}$ разбивается на пары символов $\boldsymbol{S_1, S_2}$.

$$\boldsymbol{S_1 \rightarrow k_{i_1,j_1} \quad S_2 \rightarrow k_{i_2,j_2}}$$

I.2.3 Шифр Плейфера // Playfair (Wheatstone, 1854)

Шифрование. Для каждой пары символов находим шифросимволы:

Если $i1 = i2, j1 \neq j2 \rightarrow$
$\boldsymbol{c_1 = k_{i_1, j_1+1\,(mod\,m)}}$, $\boldsymbol{c_2 = k_{i_1, j_2+1\,(mod\,m)}}$

Если $i1 \neq i2, j1 = j2 \rightarrow$
$\boldsymbol{c_1 = k_{i_1+1\,(mod\,m), j_1}}$, $\boldsymbol{c_2 = k_{i_2+1\,(mod\,m), j_1}}$

Если $i1 \neq i2, j1 \neq j2 \rightarrow$
$\boldsymbol{c_1 = k_{i_1, j_2}}$, $\boldsymbol{c_2 = k_{i_2, j_1}}$

I.2.3 Шифр Плейфера. Пример

K =

А	Б	Ґ	Д	Ж	З
В	Г	Е	Є	І	Ї
Й	К	Н	О	С	Т
Л	М	П	Р	У	Ф
Х	Ц	Щ	Ь	_	.
Ч	Ш	Ю	Я	И	,

M= ПРИВІТ_СТУДЕНТИ_КІБ

M= ПР ИВ ІТ _С ТУ ДЕ НТ И_ КІ Б.

C = РУЧІ….СЇ …….. ОЙ …..

I.2.4 Шифр Хилла (1929)

Идея→ задается $\boldsymbol{m * m}$ матрица $\boldsymbol{K}$ ключей $(\boldsymbol{m * m < n})$

$$\begin{bmatrix} \boldsymbol{k_{0,0}} & \boldsymbol{\dots} & \boldsymbol{k_{0,m}} \\ & \boldsymbol{k_{i,j}} & \\ \boldsymbol{k_{m,0}} & & \boldsymbol{k_{m,m}} \end{bmatrix} \qquad \boldsymbol{k_{i,j} = s_l \in \mathbb{Z}_n!}$$

Каждый $\boldsymbol{k_{i,j}}$ есть символ алфавита.

Размещение $\boldsymbol{k_{i,j}}$ в матрице $\boldsymbol{K}$ собственно и есть секретный ключ.

Мощность $\boldsymbol{\|K\| = (m * m)!}$

I.2.4 Шифр Хилла

Открытый текст разбивается на блоки – вектора

$$S = \begin{bmatrix} s_0 \\ s_t \\ s_{m-1} \end{bmatrix}$$ по модулю m

Шифрование

$$C = K * S \ (mod\ n)$$

Дешифрование

$$S = K^{-1} * C \ (mod\ n)$$

!!! Матрица K должна иметь мультипликативную инверсию в $\mathbb{Z}_n$

I.2.4 Шифр Хилла. Пример

$$K = \begin{bmatrix} Х & Б & У \\ Т & А & Ф \\ В & Д & Ж \end{bmatrix} = \begin{bmatrix} 24 & 2 & 22 \\ 21 & 1 & 23 \\ 3 & 5 & 8 \end{bmatrix}$$

М= ПРИВІТ_СТУДЕНТИ_КІБ

М= ПРИ ВІТ _СТ УДЕ ….

$$\begin{matrix} П \\ Р \\ И \end{matrix} \quad \begin{matrix} 18 & 8 \\ 19 & 17 \\ 10 & 12 \end{matrix} = \begin{bmatrix} 24 & 2 & 22 \\ 21 & 1 & 23 \\ 3 & 5 & 8 \end{bmatrix} * \begin{matrix} 18 & 8 \\ 19 & 7 \\ 10 & 12 \end{matrix} \quad \begin{matrix} Ж \\ Є \\ Й \end{matrix}$$

С= ЖЄЙ ЮЯМ ЕЄС РНМ ЧЮН СПЮ ОІЕ

I.2.5 Роторный шифр

Идея→ **случайным** образом задается $\boldsymbol{n}$ вектор $\boldsymbol{K}$ ключей (**ротор**) – $\boldsymbol{k_i},\ \boldsymbol{k_i \neq k_j}\ \forall i, j \in \mathbb{Z}_{\boldsymbol{n}}!$

$$t = 0, 1, 2, \dots \dots$$

$$\boldsymbol{K_0} = \begin{bmatrix} \boldsymbol{k_0} \\ \boldsymbol{k_i} \\ \boldsymbol{k_{n-1}} \end{bmatrix}$$

$$\boldsymbol{k_t = K_t[s_t]}$$

$$\boldsymbol{c_t = (k_t)}$$

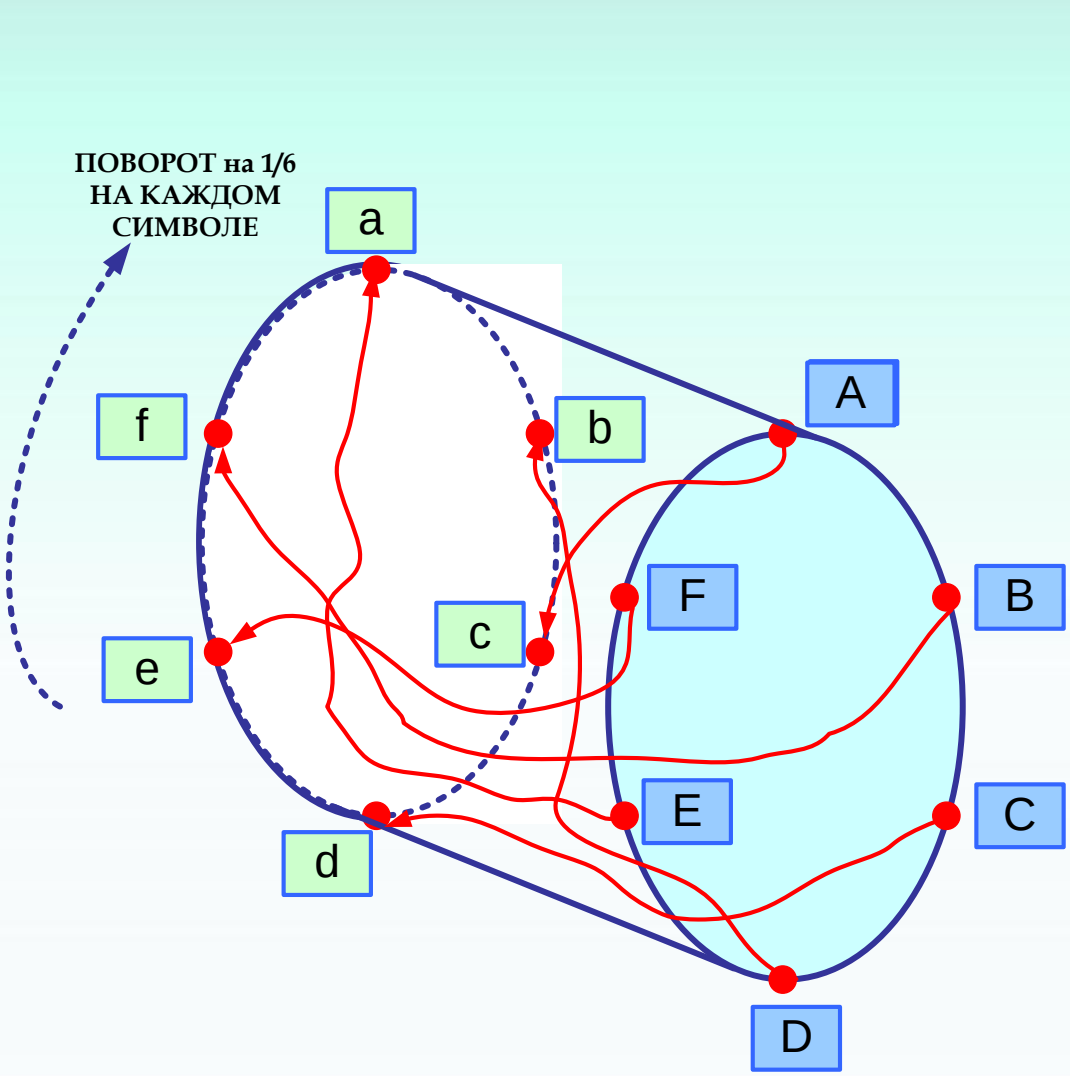
$$\boldsymbol{k_{t+1}[i] = k_t[(i+1) mod\ n]}$$

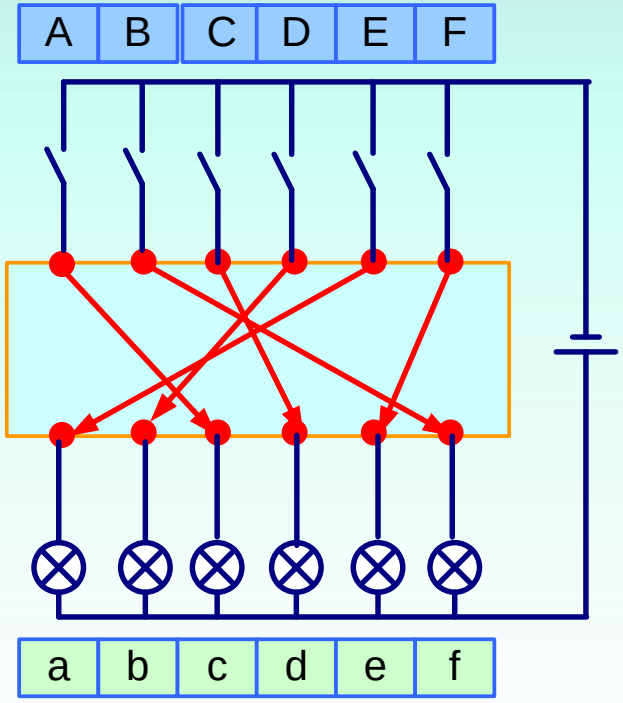
Мощность $\|\boldsymbol{K}\| = \boldsymbol{n}!$ →n=31, $\|\boldsymbol{K}\| = 8 * 10^{33}$

I.2.5 Роторный шифр

Диск Альберти “Трактат о шифрах” (Леоно Батисто Альберти, 1466 г.) — одна из первых в Европе книг, посвящённая криптоанализу.

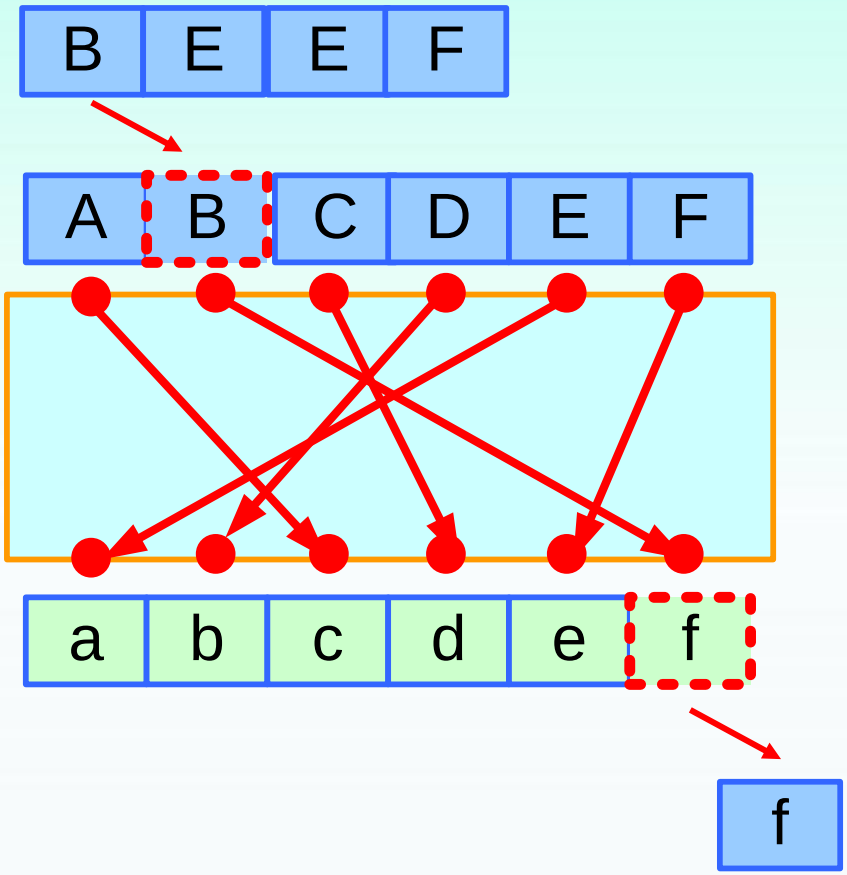
I.2.5 Роторный шифр





I.2.5 Роторный шифр

$$t = 0$$

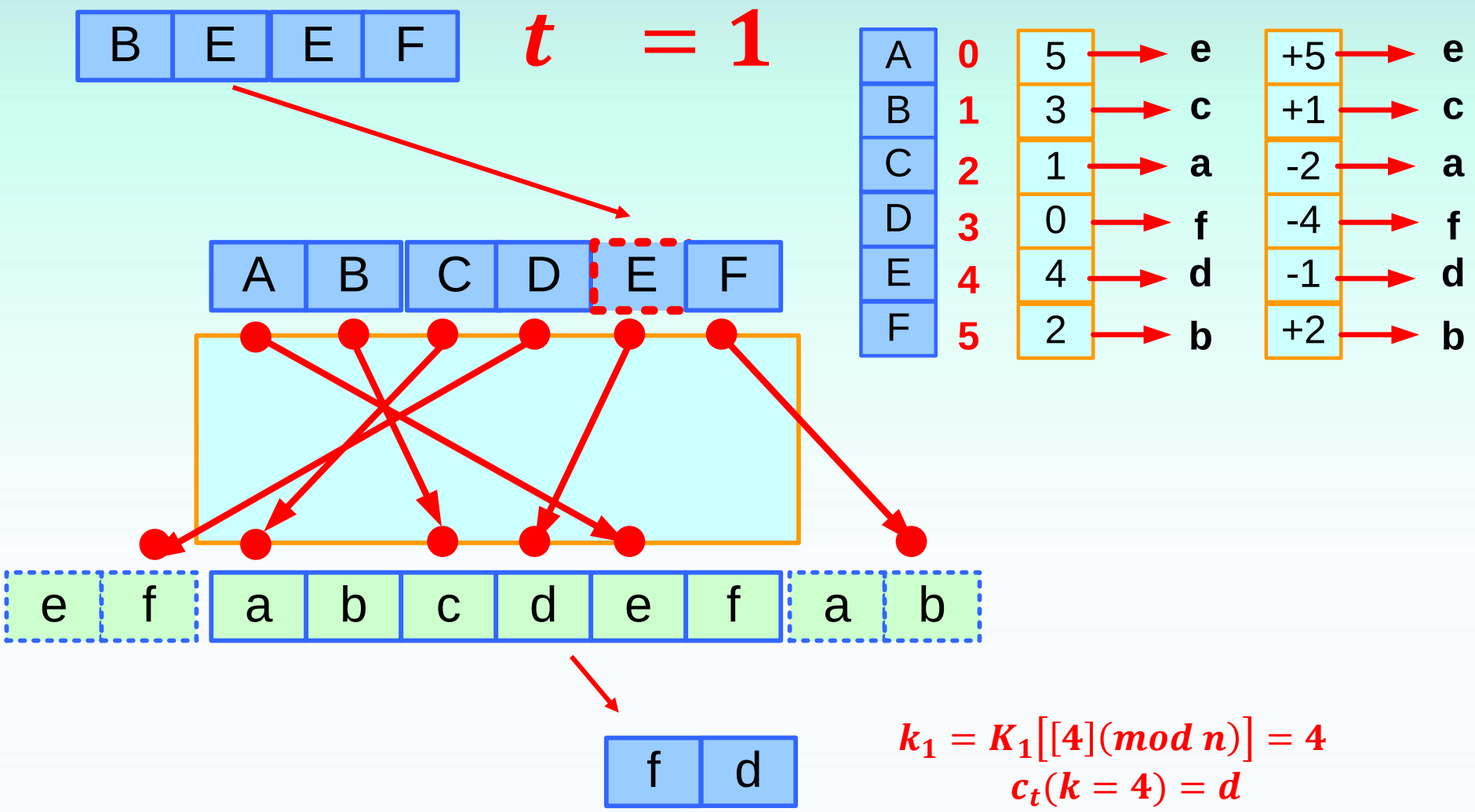


A	0	2	c	+2	c
B	1	5	f	+5	f
C	2	3	d	+1	d
D	3	1	b	-2	b
E	4	0	a	-4	a
F	5	4	e	-1	e

$$k_0 = K_0[[1](mod\ n)] = 5$$

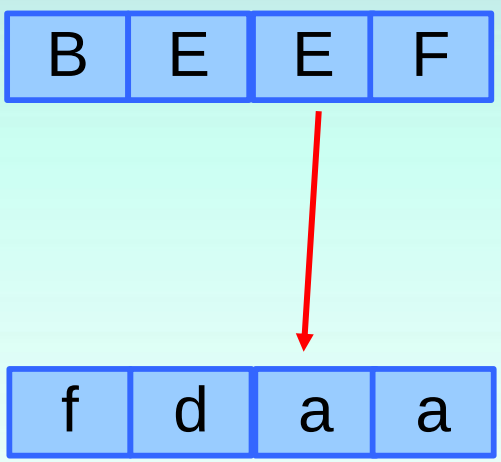
$$c_t(k = 5) = f$$

I.2.5 Роторный шифр

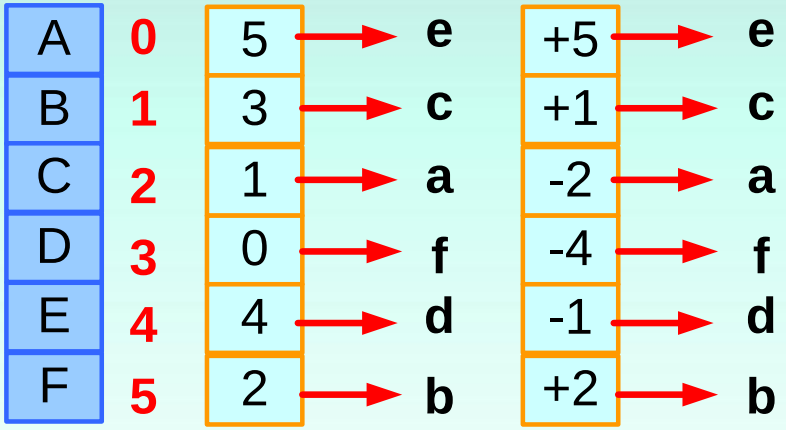


$$k_1 = K_1[[4](mod\ n)] = 4$$
$$c_t(k = 4) = d$$

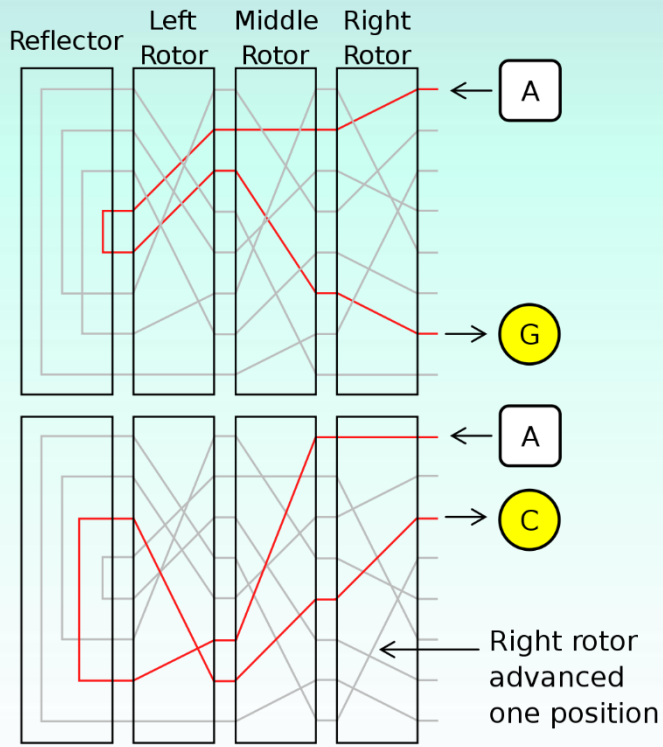
I.2.5 Роторный шифр



$t = 2, 3$



I.2.5 Роторный шифр. Энигма



- 26 букв →26!, 3 ротора →3!
- 26 стартовых позиций →26^3
- коммутационная панель (10 пар)

Мощность $\|\boldsymbol{K}\| = 2^{64}$

I.2.6 Одноразовый блокнот

Идеальный → случайным образом задается вектор $\boldsymbol{K}$ ключей с количеством элементов равным длине сообщения – $\boldsymbol{k_i \in \mathbb{Z}_n}$!

$$\boldsymbol{K} = \begin{bmatrix} \boldsymbol{k_0} \\ \boldsymbol{k_i} \\ \boldsymbol{k_L} \end{bmatrix}$$

$$\boldsymbol{k_t = k_i}$$

$$\boldsymbol{c_t = (s_t + k_t)\ mod\ n}$$

Мощность $\boldsymbol{\|K\| = L}$!

1917, Гильберт Вернам

Вопросы:

- Определите шифр с симметричным ключом.
- Поясните различие между шифром подстановки и шифром перестановки.
- В чем разница между моноалфавитными и многоалфавитными шифрами?
- Функции шифрования и дешифрования шифра Виженера. Мощность множества ключей.
- Функции шифрования и дешифрования шифра Плейфеера. Мощность множества ключей.

ЛИТЕРАТУРА

Нечаев В.И. Элементы криптографии (Основы теории защиты информации).- Учеб. пособие. – М.:, ВШ., 1999.- 109 с.

Введение в криптографию. **Под общ. ред. В.В.Ященко.** – 4-е изд., доп. М.: МЦНМО, 2012 – 348 с. ISBN 978-5-4439-0026-1

ЛИТЕРАТУРА

Венбо Мао. Современная криптография: теория и практика.—М.: Издательский дом «Вильямс», 2005.—768 с.: ил. ISSN 5-8459-0847-7 (рус.)

Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на Си. – Москва: Вильямс, 2016. 1024 с.

ЛИТЕРАТУРА

Francisco Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Cetin Kaya Koc.

Cryptographic Algorithms on Reconfigurable Hardware. - Springer, 2006.

A. Menezes, P. van Oorschot, S. Vanstone.

Handbook of Applied Cryptography.- CRC Press, 1996.

END # 6