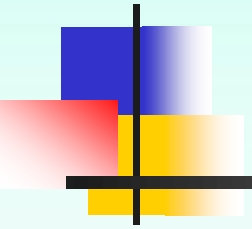
CRYPTOGRAPHY

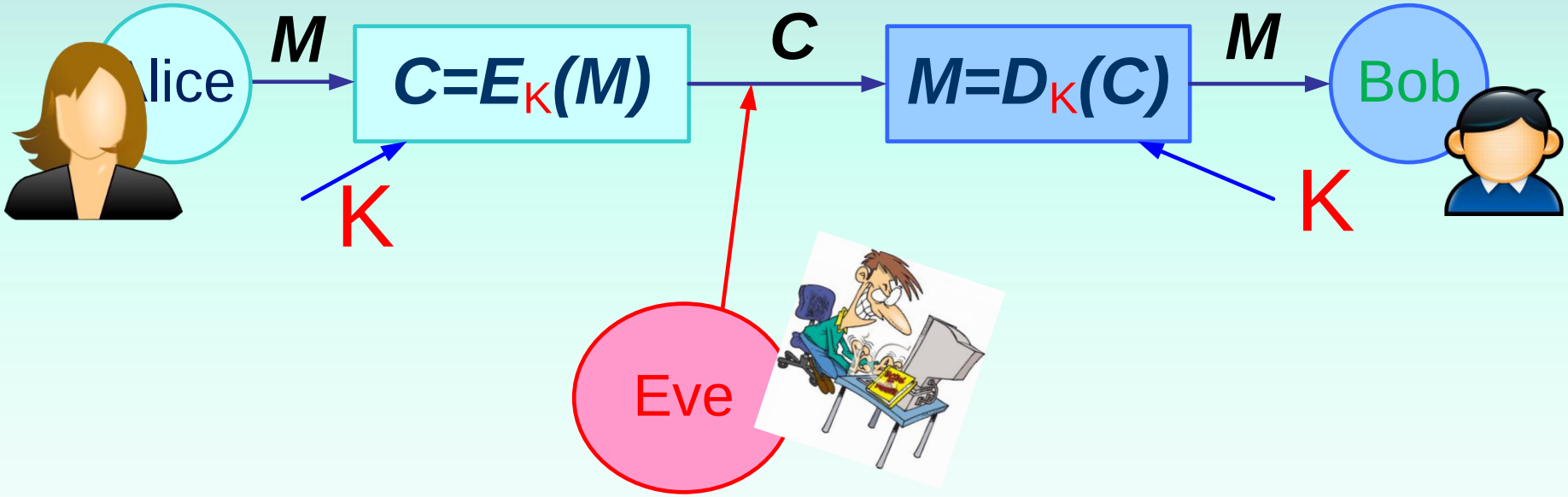


МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Лек. 7 2022 КІБ-19

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 перестановок

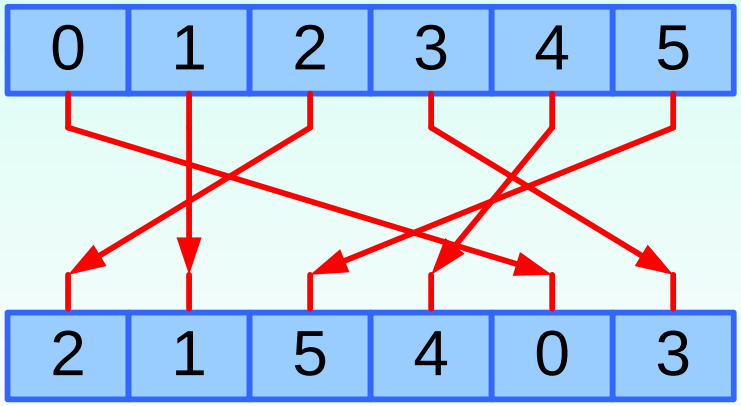
K2 = K1= K

Идея → символ не изменяется, но изменяется его положение в потоке символов.

Симметричные шифры перестановок

K2 = K1= K → таблица из 2-х строк

Первая строка таблицы → позиция символа в исходном сообщении.

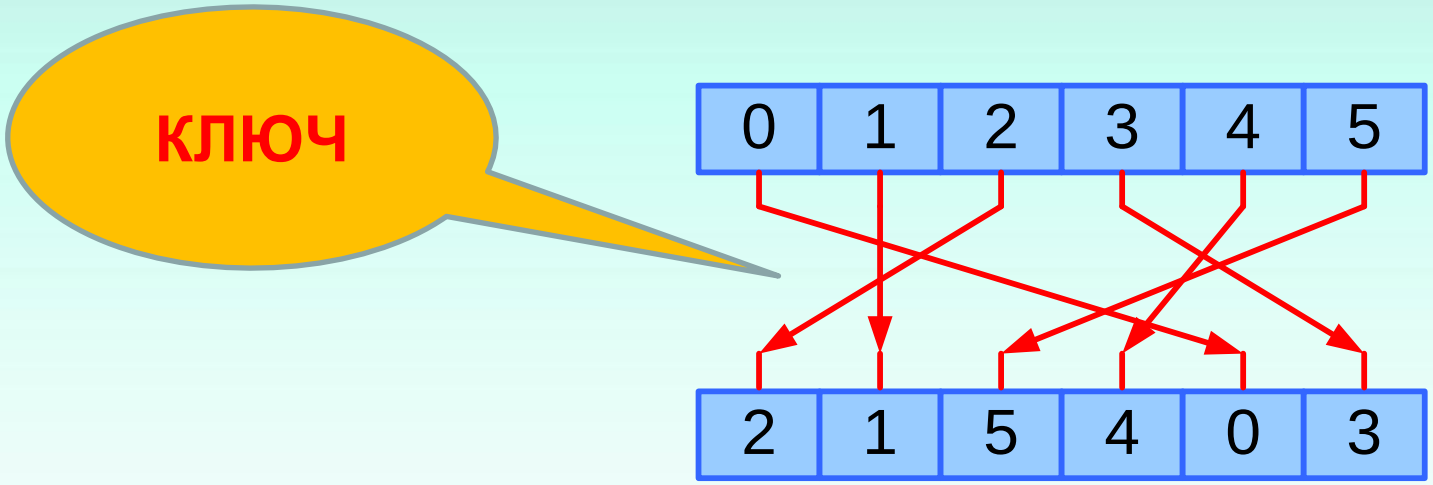


Вторая строка → позиция символа в шифрограмме.

Максимальное количество ключей для шифров перестановки равно n!, где n – длина сообщения (блока).

Симметричные шифры перестановок

Простейшая перестановка



М= ПРИВІТ _СТУДЕ НТАМ_К ІБ

С = ИРІЕПВ …..

I I.1. Бесключевые шифры

«**ИЗГОРОДЬ**» (rail fence cipher, Zig-Zag cipher)

Сообщение **mss** = $s_0, s_1, \ldots, s_t, \ldots s_L \quad s_t \in M$

П			В			_			У			Н			М			І	
	Р			І			С			Д			Т			_			Б
		И			Т			Т			Е			А			К		

М= ПРИВІТ_СТУДЕНТАМ_КІБ

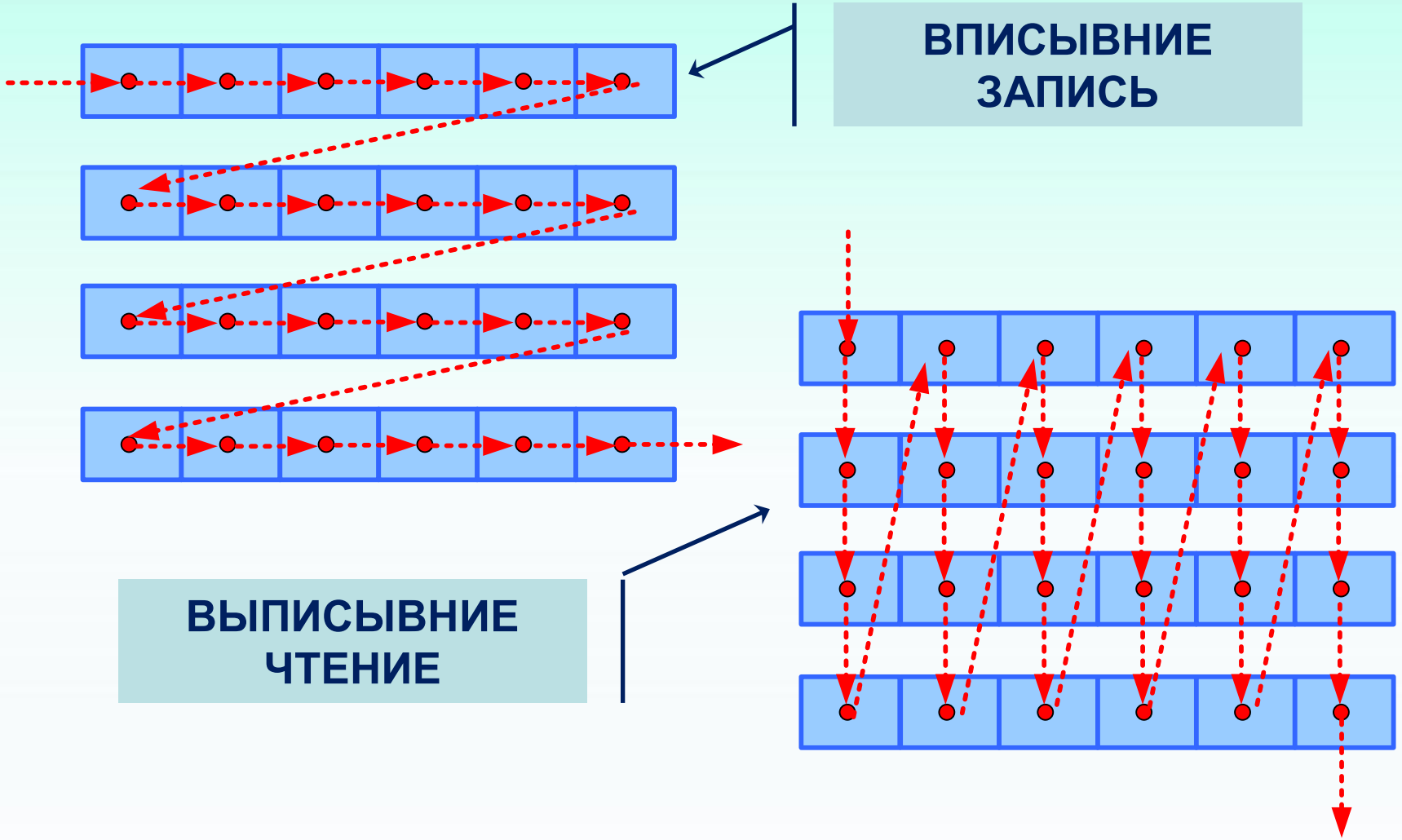
С = ПВ_УНМІРІСДТ_БИТТЕАК

Строк («рельс») q. Условие $q|L$. Количество символов в «рельсе» L/q.

Тогда $c_{\left[t\,(mod\,q)*\frac{L}{q}+\left\lfloor\frac{t}{q}\right\rfloor\right]} = s_t$.

I I.1. Бесключевые шифры

Шифры маршрутной перестановки



I I.1. Бесключевые шифры
Шифры маршрутной перестановки

Скита́ла (сцита́ла), шифр древней Спарты

L – длина сообщения
n – количество строк
m – количество столбцов

$$m = \lfloor (L-1)/n \rfloor + 1$$

І І.1. Бесключевые шифры

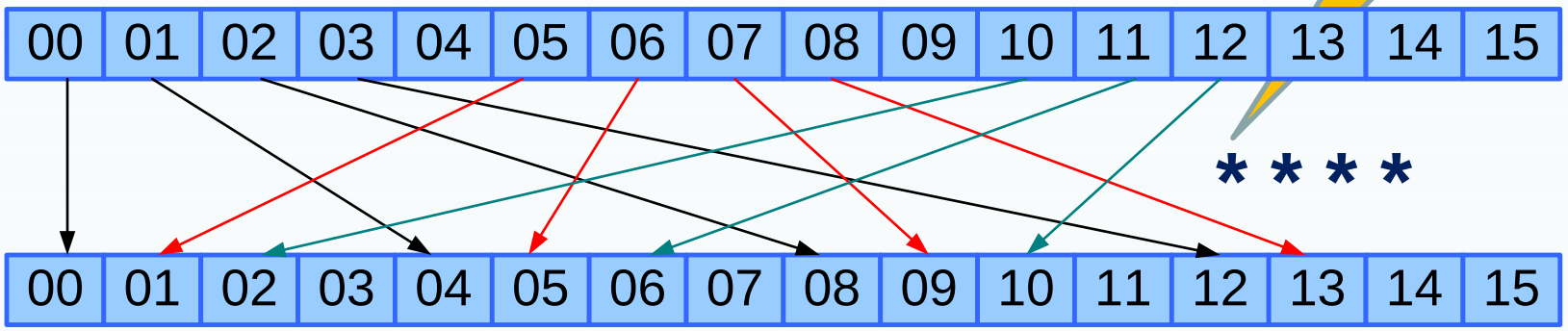
Шифры маршрутной перестановки

М= ПРИВІТ_СТУДЕНТАМ_КІБ

П	Р	И	В	І
Т	_	С	Т	У
Д	Е	Н	Т	А
М	_	К	І	Б

С = ПТДМР_Е_ИСНКВТТПУАБ

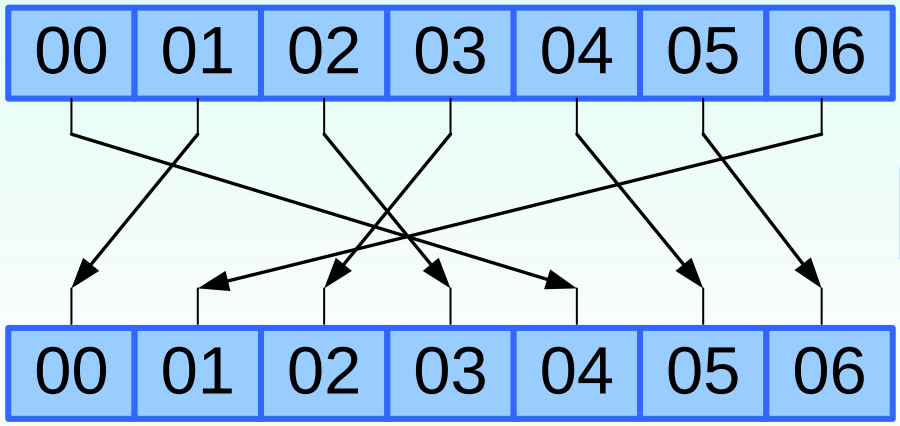
КЛЮЧ – ОПЕРАЦИЯ



II.2. Перестановка с ключом

Идея - открытый текст разбивается на блоки длиной ***q***.

Задается ***КЛЮЧ*** – **операция** перестановки длиной ***q***. Например ***q=7***



КЛЮЧ - ОПЕРАЦИЯ

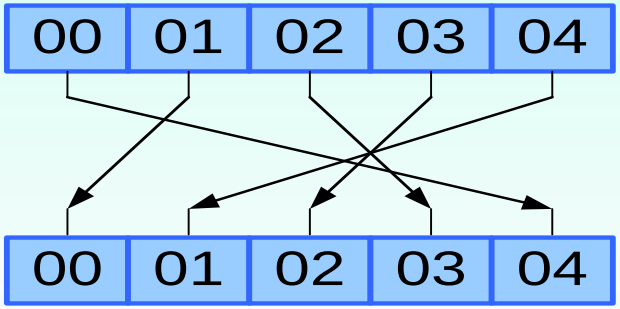
04	00	03	02	05	06	01

М= ПРИВІТ_ СТУДЕНТ АМ_КІБ

С = Р_ВИПВІ

II.2. Маршрутная перестановка с ключом

П	Р	И	В	І
Т	_	С	Т	У
Д	Е	Н	Т	А
М	_	К	І	Б



Р	І	В	И	П
_	У	Т	С	Т
Е	А	Т	Н	Д
_	Б	І	К	М

М= ПРИВІТ_СТУДЕНТАМ _КІБ

КЛЮЧ - ОПЕРАЦИЯ

С = Р_Е_ІУАБВТТІИСНКПТДМ

II.2. Маршрутная перестановка с ключом

1.ЗАПИСЬ

Р	І	В	И	П
_	У	Т	С	Т
Е	А	Т	Н	Д
_	Б	І	К	М

=

П	Р	И	В	І
Т	_	С	Т	У
Д	Е	Н	Т	А
М	_	К	І	Б

$$\times \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

2. КЛЮЧ

3.ЧТЕНИЕ

С = Р_Е_ІУАБВТТІИСНКПТДМ

Маршрут записи и маршрут чтения – 1, 3 части алгоритма

II.3. Двойная маршрутная перестановка с ключом

Многоступенчатая процедура шифрования может быть эквивалентно заменена шифром простой одинарной перестановки

Гаммирование

K2 = K1= K

По сути это **одноразовый блокнот** (аддитивный шифр) с гаммой (ключем), длина которого равна длине сообщения и выбранной случайным образом.

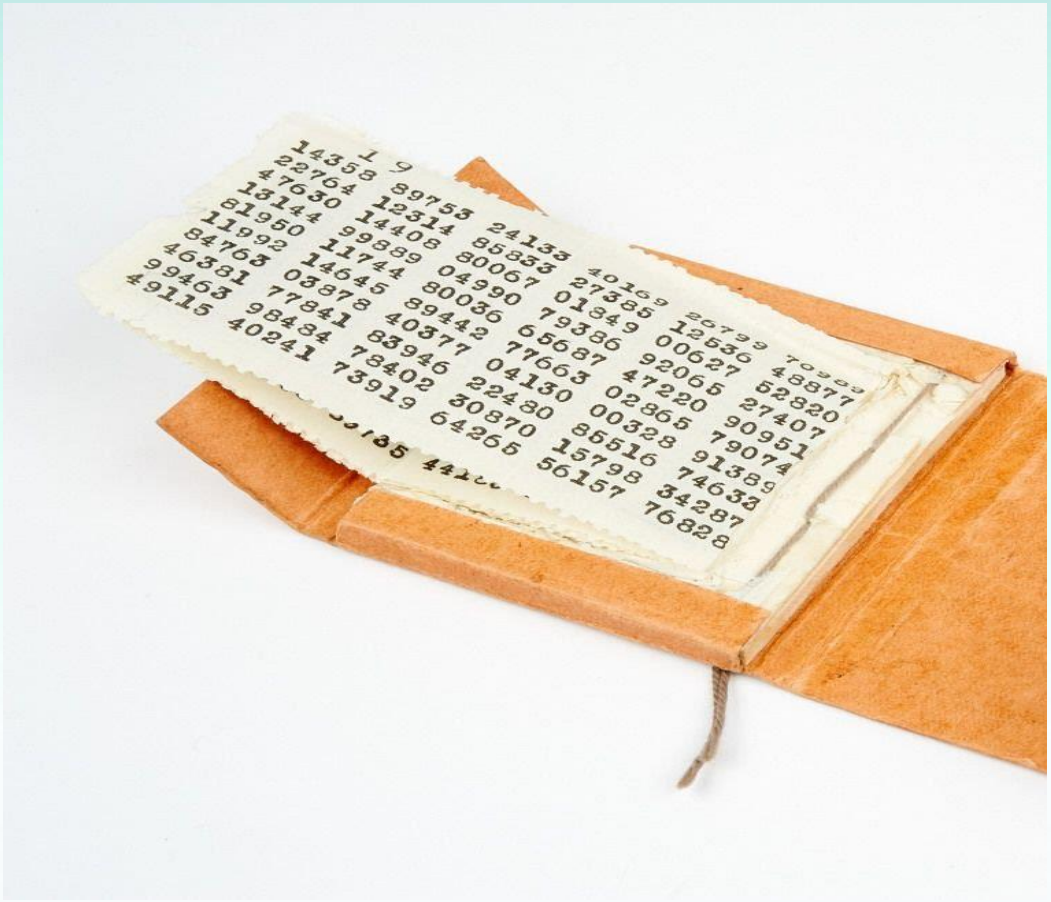
Гаммирование

Случайность распределения символов по периоду (длине) гаммы означает отсутствие закономерностей между появлением различных символов в пределах периода.

Для обеспечения абсолютной стойкости необходимо, чтобы последовательность символов в пределах периода гаммы обладала следующими свойствами:

- была случайной (отсутствовать закономерность в появлении символов гаммы);
- символы алфавита гаммы были распределены нормально (равновероятно);
- совпадала по размеру или была больше исходного открытого текста;
- применялась только один раз.

Гаммирование



Одноразовый шифровальный блокнот (СССР, ГДР, 1960-е гг.)
www.cryptomuseum.com

Вопросы:

- Поясните различие между шифром подстановки и шифром перестановки.
- Поясните идею бесключевых шифров перестановки.
- В чем заключается шифр маршрутной перестановки? Поясните алгоритм шифрования и дешифрования.
- Функции шифрования и дешифрования шифра маршрутной перестановки с ключом. 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 # 7