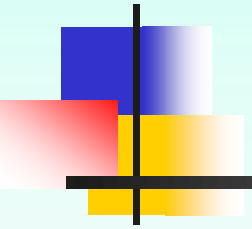
CRYPTOGRAPHY



МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

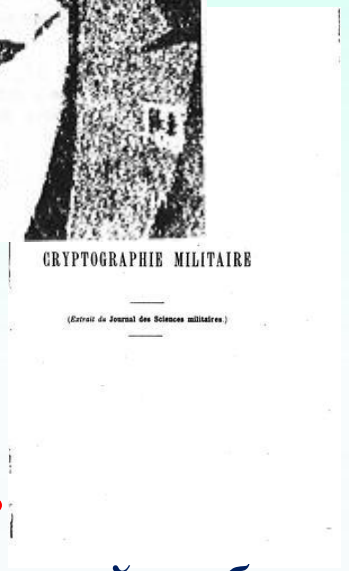
Лек. 5 2022 КІБ-19

ШИФРЫ ПОДСТАНОВОК И ПЕРЕСТАНОВОК

Принцип Керкгоффса

Керкгоффс, Огюст, «Военная криптография», 1883.

6 требований к системе безопасности.

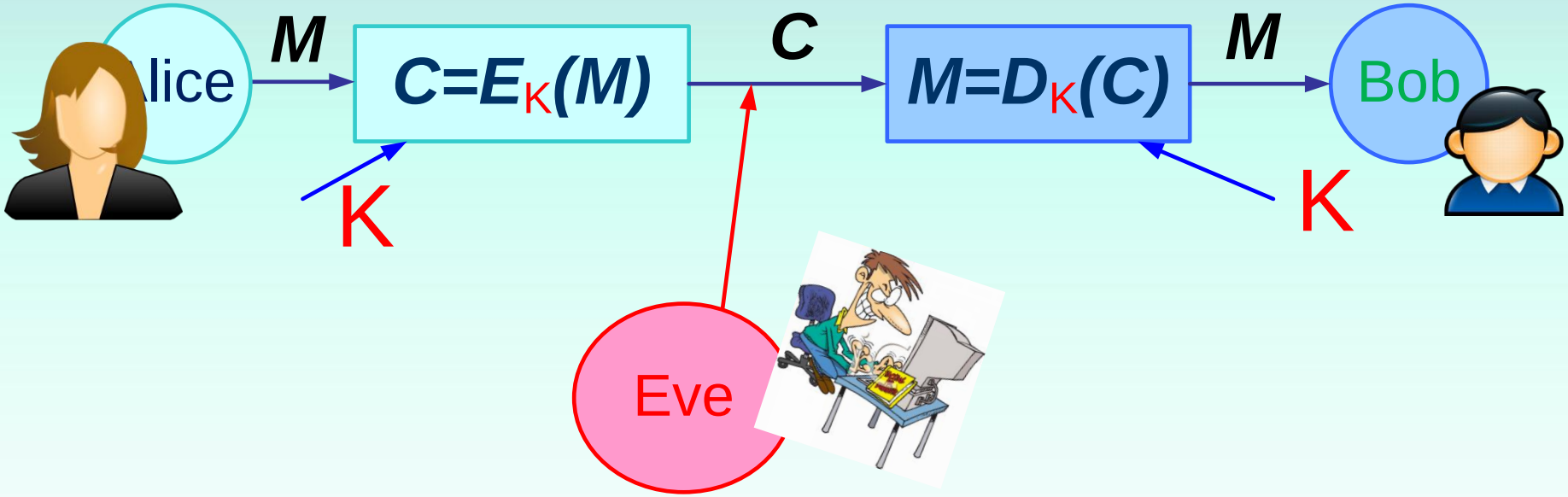


Требование 2. –Принцип

Система не должна требовать секретности, и при попадании в руки врага не должна терять надёжности.

!!! в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен быть открытым

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

Шифры подстановок

Идея → замена одного символа другим .

I.1 Моноалфавитные шифры

Идея → символ в открытом тексте всегда заменяется на некоторый другой символ в шифротексте. Не зависит от позиции символа в открытом тексте.
Отношение → один к одному!

I.1.1. Аддитивный (*сдвига, Цезаря*)

$$\boldsymbol{M = \{s|\ s \in \mathbb{Z}_n\}, C = \{c|\ c \in \mathbb{Z}_n\},}$$
$$\boldsymbol{K = \{k|\ k \in \mathbb{Z}_n^{>0}\ \}}$$
$$\boldsymbol{E(M) = (s + k)(mod\ n)}$$

I.1.1. Аддитивный. Пример.

Українська абетка

А Б В Г Ґ Д Е Є Ж З И І Ї Й К Л М Н О П Р
С Т У Ф Х Ц Ч Ш Щ Ь Ю Я
+ пробел / + апостроф (‘)

Ограничимся 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 _

$$\boldsymbol{M = \{s|\ s \in \mathbb{Z}_{31}\}, K = \{k|\ k \in \mathbb{Z}_{31}^{\geq 0}\ \}}$$

$$\boldsymbol{E(M) = (s + k)(mod\ 31)}$$

I.1.1. Аддитивный. Пример.

_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ю	Я
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

ШИФРОВАНИЕ

$$E(M) = (s + k)(mod\ 31)$$

$$c_i = (s_i + k)(mod\ 31)$$

k = 13, М=ПРИВІТ_СТУДЕНТИ_КІБ

С = _АФНХВКБВГПРЮВФКЧХМ

I.1.1. Аддитивный. Пример.

_	А	Б	В	Г	Д	Е	Є	Ж	З	И	І	Й	К	Л	М
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ю	Я
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

ДЕШИФРОВАНИЕ

$$D(C) = (c - k)(mod\ 31)$$

$$s_i = (c_i - k)(mod\ 31)$$

k = 13, C = _АФНХВКБВГПРЮВФКЧХМ

М=ПРИВІТ_СТУДЕНТИ_КІБ

I.1.1. Аддитивный.

АТАКА

Уязвим к атаке грубой силы.

$$K = \{k |\ k \in \mathbb{Z}_n^{\geq 0}\ \},$$ мощность $\|K\| = n$

В примере надо перебрать 30 ключей!

I.1.2. Мультипликативный

Шифрование:

$$M = \{s|\ s \in \mathbb{Z}_n\}, C = \{c|\ c \in \mathbb{Z}_n\},$$
$$K = \{k|\ k \in \mathbb{Z}_n^{>0}\ \}$$
$$E(M) = (s * k)(mod\ n)$$

Дешифрование:

$$K = \{k|\ k \in \mathbb{Z}_{n*}\}$$

Ключи → !!! Мультипликативно инверсны

$$D(C) = \left(c * k^{-1}\right)(mod\ n)$$

I.1.2. Мультипликативный. Пример

n=31
Имеет 30 мультипликативных инверсий
ШИФРОВАНИЕ

$$c_i = (s_i * k)(mod\ 31)$$

k = 13, М=ПРИВІТ_СТУДЕНТИ_КІБ
С = ЮІПС_ЕЙХЕРЬЩВЕПЙЧ_Є

$$s_i = \left(c_i * k^{-1}\right)(mod\ 31)$$

Уязвим к атаке грубой силы. $\|K\| = n$

I.1.3. Аффинный.

Комбинация аддитивного и мультипликативного

$$M = \{s|\ s \in \mathbb{Z}_n\}, C = \{c|\ c \in \mathbb{Z}_n\},$$
$$K = \{k|\ k \in \mathbb{Z}_n^{>0}\ \}$$

ШИФРОВАНИЕ

$$E(M) = (s * k)(mod\ n)$$
$$c_i = (s_i * k_1 + k_2)(mod\ n)$$

ДЕШИФРОВАНИЕ

$$D(C) = ((c - k_2) * k_1^{-1})(mod\ n)$$
$$s_i = \left((c_i - k_2) * k_1^{-1}\right)(mod\ n)$$

Уязвим к атаке грубой силы. $\|K\| = n * n$

I.1.4. Подстановка

Моноалфавитный шифр подстановки

Идея → каждому символу из M приписывается случайный символ из M.

$$E(M) = M \xrightarrow{K} S$$

Таблица соответствия и есть КЛЮЧ.

Например

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

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ю	Я
Й	Р	Х	Ц	Є	Г	О	М	А	В	Е	Т	Д	Ч	І

$\|K\| = n!$ **Для нас:** $31! \sim \approx 8 * 10^{33}$

I.1.4. Моноалфавитный шифр подстановки. Пример

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

Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ю	Я
Й	Р	Х	Ц	Є	Г	О	М	А	В	Е	Т	Д	Ч	І

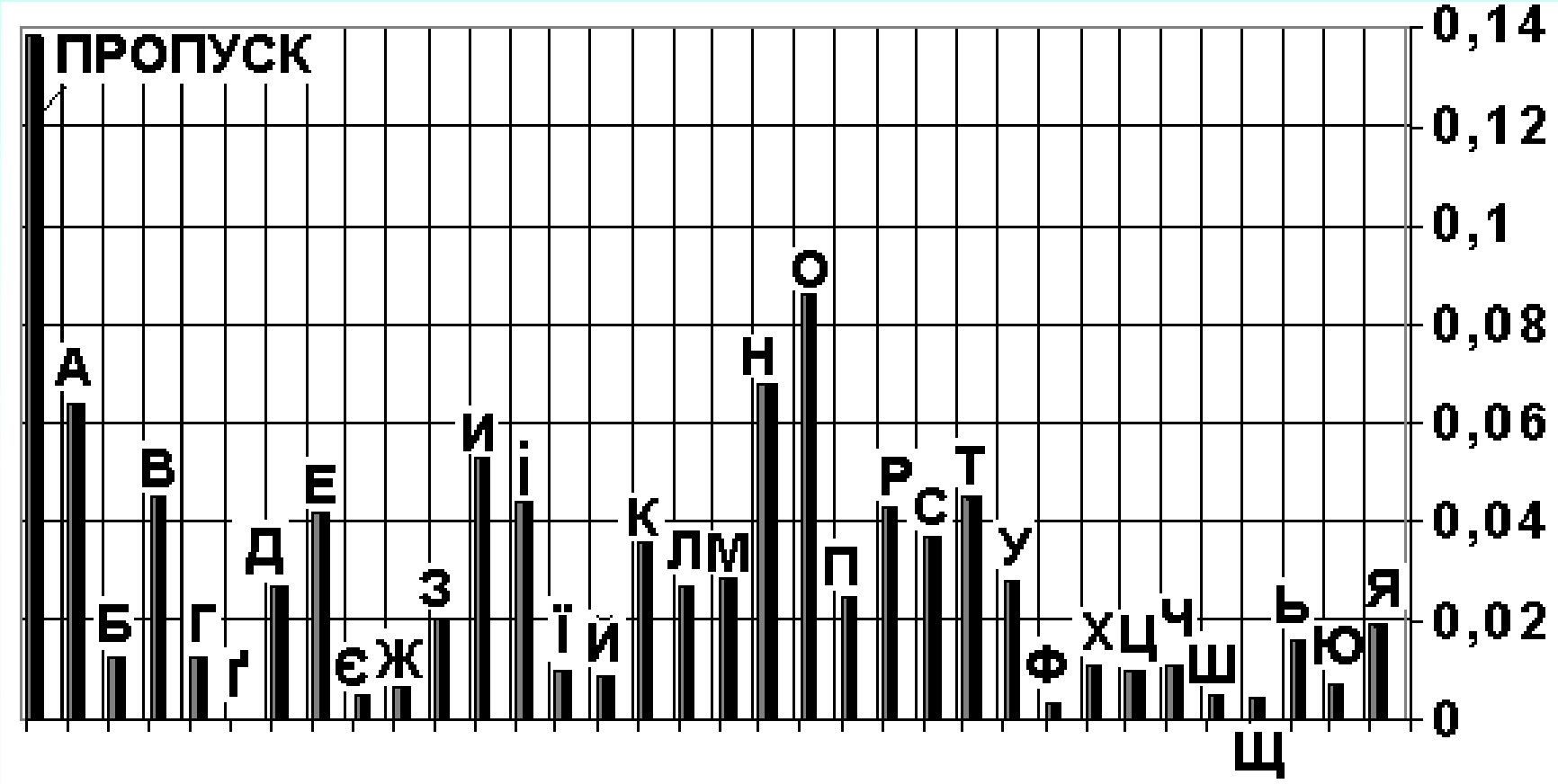
М = ПРИВІТ_СТУДЕНТИ_КІБ
С = ХЦУНКГБЄГОЗИЙГУБЩКЯ

$\|K\| = n!$ **Для нас:** $31! \sim \approx 8 * 10^{33}$

Что делать?

І.1.4. Шифр подстановки.

Середньостатистичні частоти букв української мови



І.1.4. Шифр подстановки.

Середньостатистичні частоти букв української мови

Проб	0.138	**І**	0.044	**Д**	0.027	**Г**	0.013	**Ж**	0.007
О	0.086	**Р**	0.043	**Л**	0.027	**Ч**	0.011	**Ю**	0.008
Н	0.068	**Е**	0.042	**П**	0.025	**Х**	0.011	**Є**	0.005
А	0.064	**С**	0.037	**З**	0.020	**Ї**	0.010	**Щ**	0.004
И	0.055	**К**	0.033	**Я**	0.019	**Ц**	0.010	**Ф**	0.003
В	0.046	**М**	0.029	**Ь**	0.016	**Ш**	0.005	**Ґ**	0.000
Т	0.045	**У**	0.027	**Б**	0.013	**Й**	0.009		

I.1.4. Шифр подстановки.

ПРИВІТ_СТУДЕНТИ_КІБ_ПРОШУ_ВАС_ПІДГОТУВАТИСЯ_ДО_КОНТРОЛЬНОГО _ОПРОСУ

ХЦУНКГБЄГОЗИЙГУБЩКЯБХЦРТОБН_ЄБХКЗЖРГОН_ГУЄІБЗРБЩРЙГЦРСДЙРЖРБРХЦРЄО

Символов 66

Р	0,1364
Б	0,1212
Г	0,0909

Х	0,0606
Ц	0,0606
Є	0,0606
О	0,0606

У	0,0455
Н	0,0455
К	0,0455
З	0,0455
Й	0,0455

Щ	0,0303
_	0,0303
Ж	0,0303

И	0,0152
Я	0,0152
Т	0,0152
І	0,0152
С	0,0152
Д	0,0152

І.1.4. Шифр подстановки.

ХЦУНКГБЄГОЗИЙГУБЩКЯБХЦРТОБН_ЄБХКЗЖРГОН_ГУ
ЄІБЗРБЩРЙГЦРСДЙРЖРБРХЦРЄО

1. Р→ _ Б → О Г → Н

ХЦУНКНОЄНОЗИЙНУОЩКЯОХЦ_ТООН_ЄОХКЗЖ
_НОН_НУЄІОЗ _ОЩ _ЙНЦ _СДЙ _Ж _О _ХЦ _ЄО

2. Р→ О Б → _ Г → Н

ХЦУНКН_ЄНОЗИЙНУ _ ЩКЯ _ ХЦОТО _ Н_Є _
ХКЗЖОНОН_НУЄІ _ ЗО _ЩОЙНЦОСДЙОЖО _ ОХЦОЄО

ПРИВІТ_СТУДЕНТИ_КІБ_ПРОШУ_ВАС_ПІДГОТУВАТИСЯ_Д
О_КОНТРОЛЬНОГО _ОПРОСУ

Біграми української мови

- С учетом пропуска между словами

И_ / _П / _В / О_ / А_ / НА / І_ / НО / СТ / _З / _Н

- Без учета пропуска между словами

НА / НО / СТ / ОВ / КО / РО / НИ / ЕР АН / ОМ / ПР

НА → 0,0118 НО → 0,0115 ……

І.1.4. Шифр подстановки.

3. Р→ О Б → _ Г → Н Х → П

ПЦУНКН_ЄНОЗИЙНУ _ ЩКЯ _ ПЦОТО _ Н_Є _
ПКЗЖОНОН_НУЄІ _ ЗО _ЩОЙНЦОСДЙОЖО _ ОПЦОЄО

ПРИВІТ_СТУДЕНТИ_КІБ_ПРОШУ_ВАС_ПІДГОТУВАТИСЯ_Д
О_КОНТРОЛЬНОГО _ОПРОСУ

Біграми української мови

	А	Б	В	Г	Ґ	Д	Е	Є	Ж
А	0,0000	0,0010	0,0030	0,0013	0,0000	0,0019	0,0000	0,0015	0,0008
Б	0,0014	0,0000	0,0001	0,0001	0,0000	0,0000	0,0013	0,0002	0,0000
В	**0,0068**	0,0000	0,0002	0,0000	*	0,0008	0,0017	0,0000	0,0004
Г	0,0020	0,0000	0,0000	0,0000	*	0,0000	0,0002	0,0000	0,0000
Ґ	0,0000	*	0,0000	*	*	0,0000	0,0000	0,0000	*
Д	0,0021	0,0003	0,0005	0,0001	0,0000	0,0001	0,0019	0,0000	0,0008
Е	0,0003	0,0004	0,0009	0,0006	0,0000	0,0016	0,0000	0,0000	0,0010
Є	0,0000	0,0000	0,0001	0,0000	0,0000	0,0002	0,0000	0,0000	0,0000
Ж	0,0008	0,0000	0,0000	0,0000	0,0000	0,0001	0,0021	*	0,0000
З	**0,0051**	0,0009	0,0013	0,0002	0,0000	0,0004	0,0004	0,0000	0,0000
И	0,0000	0,0003	0,0030	0,0003	0,0000	0,0007	0,0000	0,0002	0,0001
І	0,0003	0,0005	**0,0046**	0,0004	0,0000	**0,0047**	0,0000	0,0004	0,0004

О	0,0000	**0,0044**	**0,0090**	**0,0060**	0,0000	**0,0051**	0,0002	0,0003	0,0018

О	0,0013	0,0005	0,0001	0,0000	0,0022	0,0002	**0,0139**

Вопросы:

- Поясните суть «**принцип Керкгоффса**» анализа и проектирования криптографических систем.
- Функции шифрования и дешифрования аддитивного шифра. Мощность множества ключей.
- Функции шифрования и дешифрования мультипликативного шифра. Мощность множества ключей.
- Функции шифрования и дешифрования афинного шифра. Мощность множества ключей.
- Опишите шифр подстановок. Мощность множества ключей для шифра подстановок.

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 # 5