**ПРАКТИЧНІ ЗАВДАННЯ КРИПТОГРАФІЯ**

1. Створіть свій підстановочний шифр та оцініть його криптостійкість.

* абетка -> а, б, в, г, 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
* зсув -> 6
* нова абетка: ч, ш, щ, ь, ю, я, а, б, в, г, д, е, є, ж, з, и, і, ї, й, к, л, м, н, о, п, р, с, т, у, ф, х, ц
* слово -> **кібербезпека**
* зашифруємо: ждшякшявйяжч

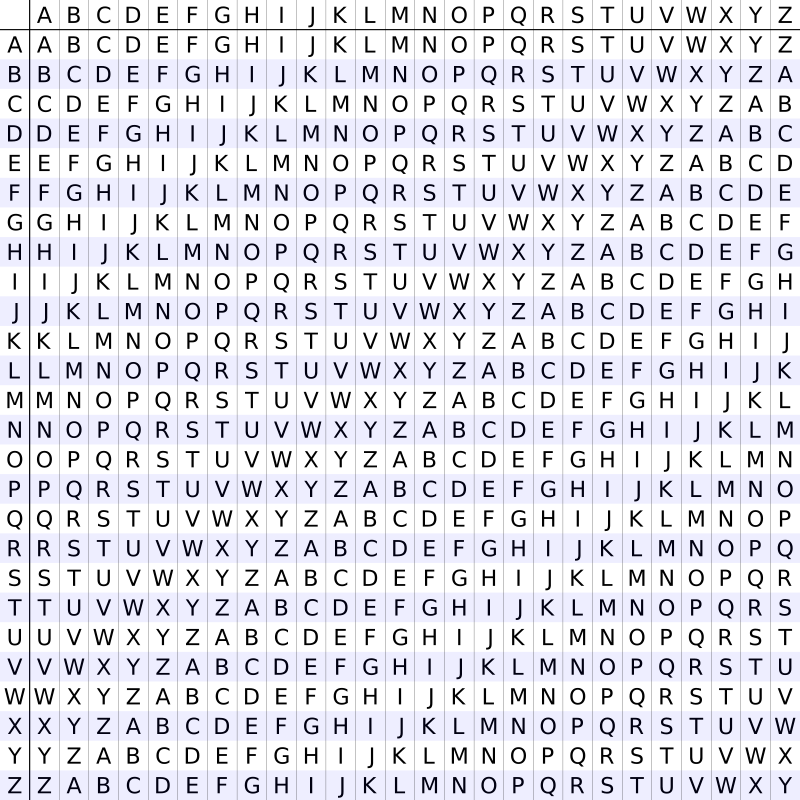
Отримали зашифроване слово: **ждшякшявйяжч ->** кібербезпека

Тепер оцінимо криптостійкість цього підстановочного шифру зі зсувом на 6 позицій. Зашифроване слово не здатне передати оригінальну структуру та частоту букв української мови. Проте, оскільки абетка має всього 33 символи, підстановочний шифр зі зсувом на 6 позицій може бути досить легко розшифрований.

Отже, криптостійкість цього підстановочного шифру є досить низькою.

1. Створіть таблицю Віженера для алфавіту англійської мови, виберіть ключ та зашифруйте повідомлення.

* горизонталь табл. - ключ
* вертикаль табл. - слово



* ключ: **good**
* слово: **information**
* зашифроване слово: **obtrxaowocq**

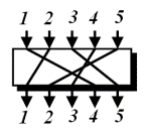
1. Створіть свій перестановочний шифр та оцініть його криптостійкість.

повтор

1. Використовуючи мультиплікативний шифр підстановки, зашифрувати повідомлення російською мовою батьківщину з ключем K = 5 (див. рис. 2.2).

<https://www.geeksforgeeks.org/what-is-multiplicative-cipher-in-cryptography/>

1. Здійснити перестановку бітів для прямого P-блоку, показаного на рис.



якщо на його вході діє послідовність: (10110)2.

10110 -> **00111**

1. Визначте послідовність із десяти чисел, що генерується методом Фібоначчі із затримкою, починаючи з kа за таких вихідних даних:

а) a = 3, b = 1, k0 = 0,6; k1 = 0,3; k2 = 0,5;

k3 = k0 - k2 = 0,6 - 0,5 = 0,1;

k4 = k1 - k3 = 0,3 - 0,1 = 0,2;

k5 = k2 - k4 = 0,5 - 0,2 = 0,3;

k6 = k3 - k5 = 0,1 - 0,3 + 1 = 0,8;

k7 = k4 - k6 = 0,2 - 0,8 + 1 = 0,4;

k8 = k5 - k7 = 0,3 - 0,4 + 1 = 0,9;

k9 = k6 - k8 = 0,8 - 0,9 + 1 = 0,9;

k10 = k7 - k9 = 0,4 - 0,9 +1 = 0,5;

k11 = k8 - k10 = 0,9 - 0,5 = 0,4;

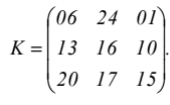
k12 = k9 - k11 = 0,9 - 0,4 = 0,5;

Послідовність: **(0,1; 0,2; 0,3; 0,8; 0,4; 0,9; 0,9; 0,5; 0,4; 0,5)**

1. Використовуючи слово 10011011(2), показати результат циркулярного (циклічного) зсуву вліво на 3 біти.

**В-дь: 11011100**

1. Нехай вихідний текст code is ready (код готовий) необхідно зашифрувати, а потім розшифрувати зашифрований текст за допомогою шифру Хілла, використовуючи ключову матрицю K (GYBNQKURP у буквеному вигляді):



<https://www.geeksforgeeks.org/hill-cipher/>

1. Зашифрувати методом розв'язання задачі про укладання рюкзака відкрите повідомлення: Обгін (14, 01, 03, 14, 13) з використанням ключа у вигляді



Елементами вектора-рядка є прості числа.

1. Значення послідовності вхідних даних у DES дорівнює: 1234567890abcdef(16). Визначити значення послідовності на виході блоку IP-перестановки.





Для визначення значення послідовності на виході блоку IP-перестановки з вхідної послідовності довжиною 64 біти, такої як "1234567890abcdef" у шістнадцятковому форматі, потрібно спочатку перевести її в бінарний формат, а потім застосувати таблицю перестановок.

➢ Вхідна послідовність (у бінарному форматі): 0001001000110100010101100111100000010011010001010101101111011111

➢ Тепер скористаємось таблицею перестановок: 58 50 42 34 26 18 10 2 60 52 44 36 28 20 12 4 62 55 47 39 31 23 15 7

➢ Переведемо у шістнадцятковий формат буде: **0x85e813540f0ab405**

1. Значення послідовності на виході E-блоку перестановки та розширення в DES дорівнює R1^e = 8a2b57d029a6(16). Значення раундового ключа: k1 = 4568581abcce(16). Визначити значення послідовності на виході операції xor функції фейстеля змішувача.

Спочатку переведемо наші значення в двійковий формат:

k1 = 4568581abcce = 10001010110100001011000000110101011110011001110

R1E = 8a2b57d029a6 = 100010100010101101010111110100000010100110100110

Тепер виконаємо операцію XOR (логічне "або-виключаюче") між двійковими значеннями k1 та R1E:

10001010110100001011000000110101011110011001110 100010100010101101010111110100000010100110100110 ------------------------------------------------------------------------ 000000001111101111100111111101010101011000111000

Тепер, переводимо в 16-річну систему: **fbe7f55638**

1. Значення послідовності на виході E-блоку перестановки та розширення в DES дорівнює R12^e = 9f3ca2bffea6(16). Значення раундового ключа: k12=c2c1e96a4bf3(16). Визначити значення послідовності на виході операції xor функції Фейстеля змішувача.

RE12 = 9f3ca2bffea6 (16)

k12 = c2c1e96a4bf3 (16)

Перетворимо їх у двійковий формат: RE12 = 100110110011110010100101101111111111111010100110 (двійковий)

k12 = 11000010110001111010100110100101001010111110011 (двійковий)

Виконаємо операцію XOR:

100110110011110010100101101111111111111010100110

XOR

11000010110001111010100110100101001010111110011 ---------------------------------------------------------------------- 010110011111101110001100000110101101110101000101

Тепер, переводимо в 16-річну систему => **5bfc630db5a5 (16)**

1. Значення послідовності на виході P-блоку прямої перестановки змішувача DES дорівнює:R3^p = 07d0a03c16. Значення послідовності: L3 = 4f73c3b3(16). Визначити значення послідовності на виході функції змішувача xor.

Представляючи значення RP3 та L3 у двійковому вигляді та використовуючи правило порозрядного підсумовування даних по модулю 2 отримаємо: 00000111110100000010100000111100

XOR

01001111011100111100001110110011

-----------------------------------------------

01001000101000111110101110001111

Перетворене значення RL на шістнадцяткове матиме вигляд RL = **48a3eb8f**

1. Для потокового алгоритму A5/1 знайдіть значення функцій:

а) f(x, y, z) = f(1, 0, 0);

б) f(x, y, z) = f(0, 1, 1);

в) f(x, y, z) = f(0, 0, 0);

г) f(x, y, z) = f(1, 1, 1).

У кожному випадку показати, скільки синхронізується лінійних регістрів зсуву.

У кожному випадку показати, скільки синхронізується лінійних регістрів зсуву.

Алгоритм A5/1 використовує три лінійних регістри зсуву з такими параметрами:

▪ Регістр 1 (19 біт): початкове значення x = (1001010100000011000)

▪ Регістр 2 (22 біти): початкове значення y=(0101100110001000101000)

▪ Регістр 3 (23 біти): початкове значення z = (11001000100001110000000)

Для генерації ключового потоку з кожного регістра витягуються біти зі старшого кінця, використовуючи многочлени зворотнього зв'язку:

▪ Регістр 1: x^19 + x^18 + x^17 + x^14 + 1

▪ Регістр 2: y^22 + y^21 + 1

▪ Регістр 3: z^23 + z^22 + x^21 + z^8 + 1

Для обчислення значення функції f(x, y, z) необхідно виконати побітову операцію XOR над відповідними бітами з трьох регістрів зсуву. Зауважимо, що значення функції залежить тільки від трьох бітів, тому лінійні регістри зсуву синхронізуються не після кожної ітерації алгоритму, а після кожних 64 кроків.

a) f(1, 0, 0) = x[18] XOR y[21] XOR z[22] = 1 XOR 0 XOR 0 = 1 Синхронізація: 64 кроки

б) f(0, 1, 1) = x[19] XOR y[22] XOR z[23] = 0 XOR 0 XOR 1 = 1 Синхронізація: 64 кроки

в) f(0, 0, 0) = x[18] XOR y[21] XOR z[22] = 1 XOR 0 XOR 0 = 1 Синхронізація: 64 кроки

г) f(1, 1, 1) = x[18] XOR y[21] XOR z[22] = 1 XOR 1 XOR 1 = 1 Синхронізація: 64 кроки

1. Визначте послідовність з десяти чисел, що генерується методом Фібоначчі із затримкою, починаючи з таких вихідних даних: a = 3, b = 1, k0 = 0,6; k1 = 0,3; k2 =0,5

повтор