

Вісник № 7

1. Як класифікують алгоритми шифрування?

Алгоритми шифрування шифрують з типом шифрування

- симетричні - у такому типі шифрування використовується один ключ для шифрування та дешифрування

- асиметричні - у такому типі шифрування ми маємо два ключа один з них - відкритий, використовується для шифрування, а інший - закритий, використовується для дешифрування.

Типи шифрування

- Блочний шифр - різновид симетричного шифру, особливістю є обробка білою деяких блоків за одну ітерацію

- Потіковий шифр - група асиметричних шифрів, які шифрують кожен символ відкритого тексту незалежно від інших символів

Бойко Вадим Віталійович
2 курс

група: 6.04195.010 21.2

спеціальність: кібербезпека
освітня програма: кібербезпека
дата: 02.06.2023

назва дисципліни:

"Теоретичні основи
криптографії"

підпис: Б

2. Пояснити сутність
адитивного шифру підстановки

Якщо в одірному шифрі
 $a=1$, тоді існує адитивний
однозначно зворотній шифр
з правилами шифрування

$$C_i = (M_i + S_i) \bmod n$$

$$M_i = (C_i + S_x) \bmod n$$

доведення здійснюється з урахуванням однієї
шифру $S_i^x = (n - S_i)$

Симетрич шифру містить в собі, що який найпростішим
легко зв'язати і одні може бути легко визначений при
знанні іншого, також для криптоаналітиків це
мож бути простий шлях для розв'язання шифру, то
якщо можна надіслати короткий повідомлення по безплати
розв'язот, тоді можна дуже легко визначити шифрування

Бойко Вадим Віталійович

2 курс

група: 6.04.125.010.21.2


спеціальність: Кібербезпека

освітня програма: Кібербезпека

дата: 02.06.2023

назва дисципліни:

"Теоретичні основи
криптографії"

підпис 

3. Переваги та недоліки ECDSA RSA

Переваги:

- забезпечення високої криптостійкості при певній довжині ключа
- простота алгоритму
- електронний підпис легко підробити
- має однукову крипту силу з зворотним підписом

Недоліки

- складність обчислень ECDSA
- необхідні великі обчислювальні ресурси
- повільність підписання документу

Переваги:


- конфіденційність і безпека інформації
- можливість ведення електронного документообігу

Григорів Вадим Віталійович
2 курс

група: 6.04.125.010.21.2

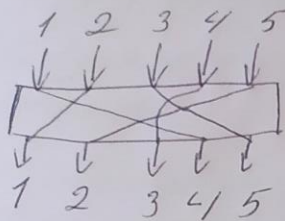
спеціальність - кибербезпека
освітня програма: кибербезпека
назва дисципліни:

"Теоретичні основи
криптографії"

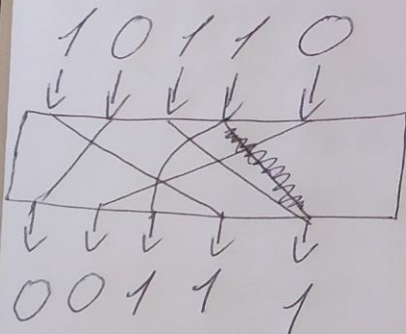
підпис 

дата: 02.06.2023

4. Здійснити перестановку
бітів для прямого P-блоку,
показано на рис.



Знайти на його виході біт
последовності $(10110)_2$



Відповідь: в результаті ми отримали зворот $(00111)_2$

Байко Вадим Віталійович
2 курс
група: 6.04.125.010.21.2
спеціальність: кібербезпека
освітня програма: кібербезпека
назва дисципліни:
"Теоретичні основи
криптографії"
дата: 02.06.2023
підпис: Б