**ЛАБОРАТОРНА РОБОТА #1**

З дисципліни «Комп'ютерна криптографія»

На тему: «Дослідження умов теоретичної секретності в симетричних криптографічних перетвореннях»

Варіант #2

|  |  |
| --- | --- |
| **Виконав**  Студент групи КВ-61м  Бондарчук М.Ю.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Прийняв**  Доцент кафедри СПСКС  Тесленко О.К.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

ЗАВДАННЯ

1. По заданих значеннях |M|, |K|, |E| створити та заповнити таблицю функції шифрування.
2. Обчислити і занести в відповідні таблиці значення апостеріорних ймовірностей початкових повідомлень, значення різниці між апостеріорними та апріорними ймовірностями початкових повідомлень, значення відношень апостеріорних ймовірностей ключів до апріорних ймовірностей відповідних початкових повідомлень при наступних умовах:
   1. при автоматичному режимі формування апріорних ймовірностей початкових повідомлень та рівно ймовірному режимі генерації ключів;
   2. при автоматичному режимі формування апріорних ймовірностей початкових повідомлень та ключів;
3. Для кожної з умов по пп. a. та b. виконати обчислення в режимі зменшеної кількості ключів.
4. Для кожної з умов по пп. a. та b. виконати обчислення при випадковій зміні значень в кожному стовпчику функції шифрування.
5. Для пп. 2, 3 та 4 вивести на друк таблицю функції шифрування, таблиці апріорних ймовірностей початкових повідомлень та ключів, таблицю апостеріорних значень початкових повідомлень, таблицю значень різниці апостеріорних та апріорних значень початкових повідомлень, таблицю відношень апостеріорної ймовірності ключів до апріорної ймовірності відповідних початкових повідомлень. Вивести на друк мотивований, з посиланням на відповідні таблиці, висновок по одержаних результатах.

ЛАТИНСЬКИЙ КВАДРАТ

Для рівноймовірних початкових повідомлень

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| f(m,k) | M1 | M2 | M3 | M4 | M5 | M6 |
| K1 | E4 | E1 | E6 | E5 | E2 | E3 |
| K2 | E1 | E5 | E2 | E4 | E3 | E6 |
| K3 | E5 | E3 | E1 | E2 | E6 | E4 |
| K4 | E6 | E4 | E5 | E3 | E1 | E2 |
| K5 | E2 | E6 | E3 | E1 | E4 | E5 |
| K6 | E3 | E2 | E4 | E6 | E5 | E1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| P(m) | M1 | M2 | M3 | M4 | M5 | M6 | Sum |
| P | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| P(k) | K1 | K2 | K3 | K4 | K5 | K6 | Sum |
| P | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Pe(m) | M1 | M2 | M3 | M4 | M5 | M6 | Sum |
| E1 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 1 |
| E2 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 1 |
| E3 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 1 |
| E4 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 1 |
| E5 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 1 |
| E6 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Pe(m) - P(m) | M1 | M2 | M3 | M4 | M5 | M6 | Sum |
| E1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Pe(k) / P(m) | E1 | E2 | E3 | E4 | E5 | E6 |
| K1 | 1 | 1 | 1 | 1 | 1 | 1 |
| K2 | 1 | 1 | 1 | 1 | 1 | 1 |
| K3 | 1 | 1 | 1 | 1 | 1 | 1 |
| K4 | 1 | 1 | 1 | 1 | 1 | 1 |
| K5 | 1 | 1 | 1 | 1 | 1 | 1 |
| K6 | 1 | 1 | 1 | 1 | 1 | 1 |

Для випадкових початкових повідомлень

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| f(m,k) | M1 | M2 | M3 | M4 | M5 | M6 |
| K1 | E3 | E1 | E5 | E2 | E4 | E6 |
| K2 | E6 | E4 | E2 | E5 | E1 | E3 |
| K3 | E1 | E3 | E4 | E6 | E2 | E5 |
| K4 | E4 | E5 | E1 | E3 | E6 | E2 |
| K5 | E2 | E6 | E3 | E4 | E5 | E1 |
| K6 | E5 | E2 | E6 | E1 | E3 | E4 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| P(m) | M1 | M2 | M3 | M4 | M5 | M6 | Sum |
| P | 0,05 | 0,24 | 0,1 | 0,34 | 0,02 | 0,24 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| P(k) | K1 | K2 | K3 | K4 | K5 | K6 | Sum |
| P | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 0,17 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Pe(m) | M1 | M2 | M3 | M4 | M5 | M6 | Sum |
| E1 | 0,05 | 0,24 | 0,1 | 0,34 | 0,02 | 0,24 | 1 |
| E2 | 0,05 | 0,24 | 0,1 | 0,34 | 0,02 | 0,24 | 1 |
| E3 | 0,05 | 0,24 | 0,1 | 0,34 | 0,02 | 0,24 | 1 |
| E4 | 0,05 | 0,24 | 0,1 | 0,34 | 0,02 | 0,24 | 1 |
| E5 | 0,05 | 0,24 | 0,1 | 0,34 | 0,02 | 0,24 | 1 |
| E6 | 0,05 | 0,24 | 0,1 | 0,34 | 0,02 | 0,24 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Pe(m) - P(m) | M1 | M2 | M3 | M4 | M5 | M6 | Sum |
| E1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Pe(k) / P(m) | E1 | E2 | E3 | E4 | E5 | E6 |
| K1 | 1 | 1 | 1 | 1 | 1 | 1 |
| K2 | 1 | 1 | 1 | 1 | 1 | 1 |
| K3 | 1 | 1 | 1 | 1 | 1 | 1 |
| K4 | 1 | 1 | 1 | 1 | 1 | 1 |
| K5 | 1 | 1 | 1 | 1 | 1 | 1 |
| K6 | 1 | 1 | 1 | 1 | 1 | 1 |

ЛАТИНСЬКИЙ ПРЯМОКУТНИК

Для рівноймовірних початкових повідомлень

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| f(m,k) | M1 | M2 | M3 | M4 | M5 | M6 | M7 |
| K1 | E4 | E1 | E6 | E3 | E7 | E5 | E2 |
| K2 | E7 | E6 | E2 | E3 | E4 | E1 | E5 |
| K3 | E7 | E6 | E3 | E1 | E5 | E2 | E4 |
| K4 | E1 | E5 | E4 | E2 | E3 | E6 | E7 |
| K5 | E1 | E2 | E6 | E4 | E7 | E3 | E5 |
| K6 | E2 | E1 | E3 | E4 | E5 | E7 | E6 |
| K7 | E6 | E5 | E2 | E1 | E3 | E4 | E7 |
| K8 | E5 | E7 | E4 | E6 | E2 | E1 | E3 |
| K9 | E2 | E4 | E7 | E5 | E1 | E3 | E6 |
| K10 | E4 | E3 | E5 | E7 | E2 | E6 | E1 |
| K11 | E6 | E3 | E5 | E7 | E1 | E4 | E2 |
| K12 | E5 | E4 | E1 | E2 | E6 | E7 | E3 |
| K13 | E3 | E7 | E1 | E5 | E6 | E2 | E4 |
| K14 | E3 | E2 | E7 | E6 | E4 | E5 | E1 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P(m) | M1 | M2 | M3 | M4 | M5 | M6 | M7 | Sum |
| P | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P(k) | K1 | K2 | K3 | K4 | K5 | K6 | K7 | K8 | K9 | K10 | K11 | K12 | K13 | K14 | Sum |
| P | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 1 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Pe(m) | M1 | M2 | M3 | M4 | M5 | M6 | M7 | Sum |
| E1 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 1 |
| E2 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 1 |
| E3 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 1 |
| E4 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 1 |
| E5 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 1 |
| E6 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 1 |
| E7 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 0,14 | 1 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Pe(m) - P(m) | M1 | M2 | M3 | M4 | M5 | M6 | M7 | Sum |
| E1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Pe(k) / P(m) | E1 | E2 | E3 | E4 | E5 | E6 | E7 |
| K1 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K2 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K3 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K4 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K6 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K7 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K8 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K9 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K10 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K11 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K12 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K13 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K14 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |

Для випадкових початкових повідомлень

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| f(m,k) | M1 | M2 | M3 | M4 | M5 | M6 | M7 |
| K1 | E6 | E1 | E2 | E4 | E5 | E3 | E7 |
| K2 | E6 | E5 | E2 | E3 | E4 | E1 | E7 |
| K3 | E7 | E3 | E1 | E5 | E6 | E4 | E2 |
| K4 | E3 | E4 | E6 | E5 | E7 | E2 | E1 |
| K5 | E2 | E1 | E3 | E4 | E6 | E7 | E5 |
| K6 | E1 | E3 | E7 | E2 | E5 | E6 | E4 |
| K7 | E4 | E2 | E7 | E6 | E1 | E5 | E3 |
| K8 | E5 | E4 | E1 | E2 | E7 | E6 | E3 |
| K9 | E3 | E2 | E5 | E7 | E4 | E1 | E6 |
| K10 | E7 | E5 | E3 | E1 | E2 | E4 | E6 |
| K11 | E4 | E6 | E5 | E3 | E1 | E7 | E2 |
| K12 | E1 | E7 | E4 | E6 | E3 | E2 | E5 |
| K13 | E2 | E7 | E6 | E1 | E3 | E5 | E4 |
| K14 | E5 | E6 | E4 | E7 | E2 | E3 | E1 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P(m) | M1 | M2 | M3 | M4 | M5 | M6 | M7 | Sum |
| P | 0,25 | 0,12 | 0,01 | 0,17 | 0,24 | 0,08 | 0,13 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P(k) | K1 | K2 | K3 | K4 | K5 | K6 | K7 | K8 | K9 | K10 | K11 | K12 | K13 | K14 | Sum |
| P | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 0,07 | 1 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Pe(m) | M1 | M2 | M3 | M4 | M5 | M6 | M7 | Sum |
| E1 | 0,25 | 0,12 | 0,01 | 0,17 | 0,24 | 0,08 | 0,13 | 1 |
| E2 | 0,25 | 0,12 | 0,01 | 0,17 | 0,24 | 0,08 | 0,13 | 1 |
| E3 | 0,25 | 0,12 | 0,01 | 0,17 | 0,24 | 0,08 | 0,13 | 1 |
| E4 | 0,25 | 0,12 | 0,01 | 0,17 | 0,24 | 0,08 | 0,13 | 1 |
| E5 | 0,25 | 0,12 | 0,01 | 0,17 | 0,24 | 0,08 | 0,13 | 1 |
| E6 | 0,25 | 0,12 | 0,01 | 0,17 | 0,24 | 0,08 | 0,13 | 1 |
| E7 | 0,25 | 0,12 | 0,01 | 0,17 | 0,24 | 0,08 | 0,13 | 1 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Pe(m) - P(m) | M1 | M2 | M3 | M4 | M5 | M6 | M7 | Sum |
| E1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| E7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Pe(k) / P(m) | E1 | E2 | E3 | E4 | E5 | E6 | E7 |
| K1 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K2 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K3 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K4 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K6 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K7 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K8 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K9 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K10 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K11 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K12 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K13 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |
| K14 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 | 0,5 |

ВИПАДОК |E| > |M|

Для рівноймовірних початкових повідомлень

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| f(m,k) | M1 | M2 | M3 | M4 |
| K1 | E2 | E1 | E3 | E5 |
| K2 | E3 | E1 | E2 | E5 |
| K3 | E4 | E2 | E1 | E3 |
| K4 | E2 | E5 | E1 | E3 |
| K5 | E1 | E2 | E3 | E4 |
| K6 | E4 | E2 | E3 | E1 |
| K7 | E2 | E5 | E1 | E4 |
| K8 | E3 | E1 | E5 | E2 |
| K9 | E3 | E4 | E2 | E1 |
| K10 | E1 | E4 | E5 | E3 |
| K11 | E1 | E3 | E4 | E2 |
| K12 | E5 | E3 | E2 | E1 |
| K13 | E5 | E3 | E4 | E2 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| P(m) | M1 | M2 | M3 | M4 | Sum |
| P | 0,25 | 0,25 | 0,25 | 0,25 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P(k) | K1 | K2 | K3 | K4 | K5 | K6 | K7 | K8 | K9 | K10 | K11 | K12 | K13 | Sum |
| P | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Pe(m) | M1 | M2 | M3 | M4 | Sum |
| E1 | 0,25 | 0,25 | 0,25 | 0,25 | 1 |
| E2 | 0,25 | 0,25 | 0,25 | 0,25 | 1 |
| E3 | 0,25 | 0,25 | 0,25 | 0,25 | 1 |
| E4 | 0,25 | 0,25 | 0,25 | 0,25 | 1 |
| E5 | 0,25 | 0,25 | 0,25 | 0,25 | 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Pe(m) - P(m) | M1 | M2 | M3 | M4 | Sum |
| E1 | 0 | 0 | 0 | 0 | 0 |
| E2 | 0 | 0 | 0 | 0 | 0 |
| E3 | 0 | 0 | 0 | 0 | 0 |
| E4 | 0 | 0 | 0 | 0 | 0 |
| E5 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Pe(k) / P(m) | E1 | E2 | E3 | E4 | E5 |
| K1 | 0,33 | 0,33 | 0,33 | 0 | 0,5 |
| K2 | 0,33 | 0,33 | 0,33 | 0 | 0,5 |
| K3 | 0,33 | 0,33 | 0,33 | 0,5 | 0 |
| K4 | 0,33 | 0,33 | 0,33 | 0 | 0,5 |
| K5 | 0,33 | 0,33 | 0,33 | 0,5 | 0 |
| K6 | 0,33 | 0,33 | 0,33 | 0,5 | 0 |
| K7 | 0,33 | 0,33 | 0 | 0,5 | 0,5 |
| K8 | 0,33 | 0,33 | 0,33 | 0 | 0,5 |
| K9 | 0,33 | 0,33 | 0,33 | 0,5 | 0 |
| K10 | 0,33 | 0 | 0,33 | 0,5 | 0,5 |
| K11 | 0,33 | 0,33 | 0,33 | 0,5 | 0 |
| K12 | 0,33 | 0,33 | 0,33 | 0 | 0,5 |
| K13 | 0 | 0,33 | 0,33 | 0,5 | 0,5 |

Для випадкових початкових повідомлень

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| f(m,k) | M1 | M2 | M3 | M4 |
| K1 | E5 | E1 | E2 | E3 |
| K2 | E4 | E1 | E2 | E3 |
| K3 | E4 | E1 | E2 | E5 |
| K4 | E2 | E4 | E3 | E1 |
| K5 | E1 | E2 | E3 | E5 |
| K6 | E5 | E2 | E3 | E4 |
| K7 | E3 | E5 | E1 | E4 |
| K8 | E3 | E4 | E1 | E2 |
| K9 | E3 | E5 | E1 | E2 |
| K10 | E2 | E3 | E5 | E1 |
| K11 | E1 | E3 | E5 | E2 |
| K12 | E2 | E3 | E4 | E1 |
| K13 | E1 | E2 | E4 | E3 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| P(m) | M1 | M2 | M3 | M4 | Sum |
| P | 0,26 | 0,11 | 0,25 | 0,39 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P(k) | K1 | K2 | K3 | K4 | K5 | K6 | K7 | K8 | K9 | K10 | K11 | K12 | K13 | Sum |
| P | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 0,08 | 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Pe(m) | M1 | M2 | M3 | M4 | Sum |
| E1 | 0,26 | 0,11 | 0,25 | 0,39 | 1,00 |
| E2 | 0,26 | 0,11 | 0,25 | 0,39 | 1,00 |
| E3 | 0,26 | 0,11 | 0,25 | 0,39 | 1,00 |
| E4 | 0,26 | 0,11 | 0,25 | 0,39 | 1,00 |
| E5 | 0,26 | 0,11 | 0,25 | 0,39 | 1,00 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Pe(m) - P(m) | M1 | M2 | M3 | M4 | Sum |
| E1 | 0 | 0 | 0 | 0 | 0 |
| E2 | 0 | 0 | 0 | 0 | 0 |
| E3 | 0 | 0 | 0 | 0 | 0 |
| E4 | 0 | 0 | 0 | 0 | 0 |
| E5 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Pe(k) / P(m) | E1 | E2 | E3 | E4 | E5 |
| K1 | 0,33 | 0,33 | 0,33 | 0,00 | 0,50 |
| K2 | 0,33 | 0,33 | 0,33 | 0,50 | 0,00 |
| K3 | 0,33 | 0,33 | 0,00 | 0,50 | 0,50 |
| K4 | 0,33 | 0,33 | 0,33 | 0,50 | 0,00 |
| K5 | 0,33 | 0,33 | 0,33 | 0,00 | 0,50 |
| K6 | 0,00 | 0,33 | 0,33 | 0,50 | 0,50 |
| K7 | 0,33 | 0,00 | 0,33 | 0,50 | 0,50 |
| K8 | 0,33 | 0,33 | 0,33 | 0,50 | 0,00 |
| K9 | 0,33 | 0,33 | 0,33 | 0,00 | 0,50 |
| K10 | 0,33 | 0,33 | 0,33 | 0,00 | 0,50 |
| K11 | 0,33 | 0,33 | 0,33 | 0,00 | 0,50 |
| K12 | 0,33 | 0,33 | 0,33 | 0,50 | 0,00 |
| K13 | 0,33 | 0,33 | 0,33 | 0,50 | 0,00 |