Київський національний університет імені Тараса Шевченка
Факультет комп’ютерних наук та кібернетики
Кафедра інтелектуальних програмних систем
Математичні основи захисту інформації

Лабораторна робота №8
“Блокове шифрування”

Виконали студенти 3-го курсу
Групи ІПС-32

Роботу виконали:
Група 1
Ольховатий Ігор
Ковальов Володимир
Тряско Софія
Група 2
Цілинко Олександр
Бондар Юлія
Волик Артем

Київ 2023

Завдання:

Поділитись на 2 групи, кожна бере повідомлення, яке було запропоноване викладачем і шифрує його за допомогою блокового способу шифрування на основі груп підстановок. Потім обмінятись цими повідомленнями і розшифрувати їх.

Шифрування група 1

Маємо повідомлення

“it was disclosed yesterday that several informal but direct contacts have been made with political representives of the viet cong in moscow”

Видалимо всі пробіли і замінимо всі букви на їх великі відповідники

ITWASDISCLOSEDYESTERDAYTHATSEVERALINFORMALBUTDIRECTCONTACTSHAVE BEENMADEWITHPOLITICALREPRESENTIVESOFTHEVIETCONGINMOSCOW

Розглянемо наступні параметри шифрування

$t = 4, j_1 = 5, j_2 = 7, j_3 = 2, j_4 = 19$

Отже маємо наступні функції підстановок:

$x_1(k) = k + 5 \, mod \, 26$

$x_2(k) = k + 7 \, mod \, 26$

$x_3(k) = k + 2 \, mod \, 26$

$x_4(k) = k + 19 \, mod \, 26$

Тепер розбиваємо речення на блоки по 4 символи і застосовуємо функції підстановок для кожного блоку:

Блок: ITWA

x1(8)=8+5 mod 26 =10(N)

x2(19)=19+7 mod 26 =0(A)

x3(22)=22+2 mod 26 =24(Y)

x4(22)=0+19 mod 26 =19(T)

Блок: SDIS

x1(18)=18+5 mod 26 =20(X)

x2(3)=3+7 mod 26 =10(K)

x3(8)=8+2 mod 26 =10(K)

x4(8)=18+19 mod 26 =11(L)

Блок: CLOS

x1(2)=2+5 mod 26 =4(H)

x2(11)=11+7 mod 26 =18(S)

x3(14)=14+2 mod 26 =16(Q)

x4(14)=18+19 mod 26 =11(L)

Блок: EDYE

x1(4)=4+5 mod 26 =6(J)

x2(3)=3+7 mod 26 =10(K)

x3(24)=24+2 mod 26 =0(A)

x4(24)=4+19 mod 26 =23(X)

Блок: STER
x1(18)=18+5 mod 26 =20(X)
x2(19)=19+7 mod 26 =0(A)
x3(4)=4+2 mod 26 =6(G)
x4(4)=17+19 mod 26 =10(K)
Блок: DAYT
x1(3)=3+5 mod 26 =5(I)
x2(0)=0+7 mod 26 =7(H)
x3(24)=24+2 mod 26 =0(A)
x4(24)=19+19 mod 26 =12(M)
Блок: HATS
x1(7)=7+5 mod 26 =9(M)
x2(0)=0+7 mod 26 =7(H)
x3(19)=19+2 mod 26 =21(V)
x4(19)=18+19 mod 26 =11(L)
Блок: EVER
x1(4)=4+5 mod 26 =6(J)
x2(21)=21+7 mod 26 =2(C)
x3(4)=4+2 mod 26 =6(G)
x4(4)=17+19 mod 26 =10(K)
Блок: ALIN
x1(0)=0+5 mod 26 =2(F)
x2(11)=11+7 mod 26 =18(S)
x3(8)=8+2 mod 26 =10(K)
x4(8)=13+19 mod 26 =6(G)
Блок: FORM
x1(5)=5+5 mod 26 =7(K)
x2(14)=14+7 mod 26 =21(V)
x3(17)=17+2 mod 26 =19(T)
x4(17)=12+19 mod 26 =5(F)
Блок: ALBU
x1(0)=0+5 mod 26 =2(F)
x2(11)=11+7 mod 26 =18(S)
x3(1)=1+2 mod 26 =3(D)
x4(1)=20+19 mod 26 =13(N)
Блок: TDIR
x1(19)=19+5 mod 26 =21(Y)
x2(3)=3+7 mod 26 =10(K)
x3(8)=8+2 mod 26 =10(K)
x4(8)=17+19 mod 26 =10(K)
Блок: ECTC
x1(4)=4+5 mod 26 =6(J)
x2(2)=2+7 mod 26 =9(J)
x3(19)=19+2 mod 26 =21(V)
x4(19)=2+19 mod 26 =21(V)
Блок: ONTA
x1(14)=14+5 mod 26 =16(T)
x2(13)=13+7 mod 26 =20(U)

x3(19)=19+2 mod 26 =21(V)
x4(19)=0+19 mod 26 =19(T)
Блок: CTSH
x1(2)=2+5 mod 26 =4(H)
x2(19)=19+7 mod 26 =0(A)
x3(18)=18+2 mod 26 =20(U)
x4(18)=7+19 mod 26 =0(A)
Блок: AVEB
x1(0)=0+5 mod 26 =2(F)
x2(21)=21+7 mod 26 =2(C)
x3(4)=4+2 mod 26 =6(G)
x4(4)=1+19 mod 26 =20(U)
Блок: EENM
x1(4)=4+5 mod 26 =6(J)
x2(4)=4+7 mod 26 =11(L)
x3(13)=13+2 mod 26 =15(P)
x4(13)=12+19 mod 26 =5(F)
Блок: ADEW
x1(0)=0+5 mod 26 =2(F)
x2(3)=3+7 mod 26 =10(K)
x3(4)=4+2 mod 26 =6(G)
x4(4)=22+19 mod 26 =15(P)
Блок: ITHP
x1(8)=8+5 mod 26 =10(N)
x2(19)=19+7 mod 26 =0(A)
x3(7)=7+2 mod 26 =9(J)
x4(7)=15+19 mod 26 =8(I)
Блок: OLIT
x1(14)=14+5 mod 26 =16(T)
x2(11)=11+7 mod 26 =18(S)
x3(8)=8+2 mod 26 =10(K)
x4(8)=19+19 mod 26 =12(M)
Блок: ICAL
x1(8)=8+5 mod 26 =10(N)
x2(2)=2+7 mod 26 =9(J)
x3(0)=0+2 mod 26 =2(C)
x4(0)=11+19 mod 26 =4(E)
Блок: REPR
x1(17)=17+5 mod 26 =19(W)
x2(4)=4+7 mod 26 =11(L)
x3(15)=15+2 mod 26 =17(R)
x4(15)=17+19 mod 26 =10(K)
Блок: ESEN
x1(4)=4+5 mod 26 =6(J)
x2(18)=18+7 mod 26 =25(Z)
x3(4)=4+2 mod 26 =6(G)
x4(4)=13+19 mod 26 =6(G)
Блок: TIVE

x1(19)=19+5 mod 26 =21(Y)
x2(8)=8+7 mod 26 =15(P)
x3(21)=21+2 mod 26 =23(X)
x4(21)=4+19 mod 26 =23(X)
Блок: SOFT
x1(18)=18+5 mod 26 =20(X)
x2(14)=14+7 mod 26 =21(V)
x3(5)=5+2 mod 26 =7(H)
x4(5)=19+19 mod 26 =12(M)
Блок: HEVI
x1(7)=7+5 mod 26 =9(M)
x2(4)=4+7 mod 26 =11(L)
x3(21)=21+2 mod 26 =23(X)
x4(21)=8+19 mod 26 =1(B)
Блок: ETCO
x1(4)=4+5 mod 26 =6(J)
x2(19)=19+7 mod 26 =0(A)
x3(2)=2+2 mod 26 =4(E)
x4(2)=14+19 mod 26 =7(H)
Блок: NGIN
x1(13)=13+5 mod 26 =15(S)
x2(6)=6+7 mod 26 =13(N)
x3(8)=8+2 mod 26 =10(K)
x4(8)=13+19 mod 26 =6(G)
Блок: MOSC
x1(12)=12+5 mod 26 =14(R)
x2(14)=14+7 mod 26 =21(V)
x3(18)=18+2 mod 26 =20(U)
x4(18)=2+19 mod 26 =21(V)

Отже зашифрованний текст має вигляд

NAYT XKKL HSQL JKAX XAGK IHAM MHVL JCGK FSKG KVTF FSDN YKKK JJVV TUVT HAUA FCGU JLPF FKGP NAJI TSKM NJCE WLRK JZGG YPXX XVHM MLXB JAEH SNKG RVUV

Дешифрування група 2

Маємо вхідні параметри $t = 4$, $j_1 = 5$, $j_2 = 7$, $j_3 = 2$, $j_4 = 19$

Та вхідний шифротекст
NAYT XKKL HSQL JKAX XAGK IHAM MHVL JCGK FSKG KVTF FSDN YKKK JJVV TUVT HAUA FCGU JLPF FKGP NAJI TSKM NJCE WLRK JZGG YPXX XVHM MLXB JAEH SNKG RVUV

Обернені функції підстановок:

$x_1^{-1}(k) = (k - j_1) \, mod \, 26$

$$x_2^{-1}(k) = (k - j_2) \; mod \; 26$$
$$x_3^{-1}(k) = (k - j_3) \; mod \; 26$$
$$x_4^{-1}(k) = (k - j_4) \; mod \; 26$$

Тепер розшифруємо кожен блок:
Блок: NAYT
x1(13)=13-5 mod 33 =8(L)
x2(0)=0-7 mod 33 =19(T)
x3(24)=24-2 mod 33 =22(W)
x4(24)=24-19 mod 33 =5(F)
Блок: XKKL
x1(23)=23-5 mod 33 =18(V)
x2(10)=10-7 mod 33 =3(D)
x3(10)=10-2 mod 33 =8(I)
x4(10)=10-19 mod 33 =17(R)
Блок: HSQL
x1(7)=7-5 mod 33 =2(F)
x2(18)=18-7 mod 33 =11(L)
x3(16)=16-2 mod 33 =14(O)
x4(16)=16-19 mod 33 =23(X)
Блок: JKAX
x1(9)=9-5 mod 33 =4(H)
x2(10)=10-7 mod 33 =3(D)
x3(0)=0-2 mod 33 =24(Y)
x4(0)=0-19 mod 33 =7(H)
Блок: XAGK
x1(23)=23-5 mod 33 =18(V)
x2(0)=0-7 mod 33 =19(T)
x3(6)=6-2 mod 33 =4(E)
x4(6)=6-19 mod 33 =13(N)
Блок: IHAM
x1(8)=8-5 mod 33 =3(G)
x2(7)=7-7 mod 33 =0(A)
x3(0)=0-2 mod 33 =24(Y)
x4(0)=0-19 mod 33 =7(H)
Блок: MHVL
x1(12)=12-5 mod 33 =7(K)
x2(7)=7-7 mod 33 =0(A)
x3(21)=21-2 mod 33 =19(T)
x4(21)=21-19 mod 33 =2(C)
Блок: JCGK
x1(9)=9-5 mod 33 =4(H)
x2(2)=2-7 mod 33 =21(V)
x3(6)=6-2 mod 33 =4(E)
x4(6)=6-19 mod 33 =13(N)
Блок: FSKG

x1(5)=5-5 mod 33 =0(D)
x2(18)=18-7 mod 33 =11(L)
x3(10)=10-2 mod 33 =8(I)
x4(10)=10-19 mod 33 =17(R)
Блок: KVTF
x1(10)=10-5 mod 33 =5(I)
x2(21)=21-7 mod 33 =14(O)
x3(19)=19-2 mod 33 =17(R)
x4(19)=19-19 mod 33 =0(A)
Блок: FSDN
x1(5)=5-5 mod 33 =0(D)
x2(18)=18-7 mod 33 =11(L)
x3(3)=3-2 mod 33 =1(B)
x4(3)=3-19 mod 33 =10(K)
Блок: YKKK
x1(24)=24-5 mod 33 =19(W)
x2(10)=10-7 mod 33 =3(D)
x3(10)=10-2 mod 33 =8(I)
x4(10)=10-19 mod 33 =17(R)
Блок: JJVV
x1(9)=9-5 mod 33 =4(H)
x2(9)=9-7 mod 33 =2(C)
x3(21)=21-2 mod 33 =19(T)
x4(21)=21-19 mod 33 =2(C)
Блок: TUVT
x1(19)=19-5 mod 33 =14(R)
x2(20)=20-7 mod 33 =13(N)
x3(21)=21-2 mod 33 =19(T)
x4(21)=21-19 mod 33 =2(C)
Блок: HAUA
x1(7)=7-5 mod 33 =2(F)
x2(0)=0-7 mod 33 =19(T)
x3(20)=20-2 mod 33 =18(S)
x4(20)=20-19 mod 33 =1(B)
Блок: FCGU
x1(5)=5-5 mod 33 =0(D)
x2(2)=2-7 mod 33 =21(V)
x3(6)=6-2 mod 33 =4(E)
x4(6)=6-19 mod 33 =13(N)
Блок: JLPF
x1(9)=9-5 mod 33 =4(H)
x2(11)=11-7 mod 33 =4(E)
x3(15)=15-2 mod 33 =13(N)
x4(15)=15-19 mod 33 =22(W)
Блок: FKGP
x1(5)=5-5 mod 33 =0(D)
x2(10)=10-7 mod 33 =3(D)
x3(6)=6-2 mod 33 =4(E)

x4(6)=6-19 mod 33 =13(N)
Блок: NAJI
x1(13)=13-5 mod 33 =8(L)
x2(0)=0-7 mod 33 =19(T)
x3(9)=9-2 mod 33 =7(H)
x4(9)=9-19 mod 33 =16(Q)
Блок: TSKM
x1(19)=19-5 mod 33 =14(R)
x2(18)=18-7 mod 33 =11(L)
x3(10)=10-2 mod 33 =8(I)
x4(10)=10-19 mod 33 =17(R)
Блок: NJCE
x1(13)=13-5 mod 33 =8(L)
x2(9)=9-7 mod 33 =2(C)
x3(2)=2-2 mod 33 =0(A)
x4(2)=2-19 mod 33 =9(J)
Блок: WLRK
x1(22)=22-5 mod 33 =17(U)
x2(11)=11-7 mod 33 =4(E)
x3(17)=17-2 mod 33 =15(P)
x4(17)=17-19 mod 33 =24(Y)
Блок: JZGG
x1(9)=9-5 mod 33 =4(H)
x2(25)=25-7 mod 33 =18(S)
x3(6)=6-2 mod 33 =4(E)
x4(6)=6-19 mod 33 =13(N)
Блок: YPXX
x1(24)=24-5 mod 33 =19(W)
x2(15)=15-7 mod 33 =8(I)
x3(23)=23-2 mod 33 =21(V)
x4(23)=23-19 mod 33 =4(E)
Блок: XVHM
x1(23)=23-5 mod 33 =18(V)
x2(21)=21-7 mod 33 =14(O)
x3(7)=7-2 mod 33 =5(F)
x4(7)=7-19 mod 33 =14(O)
Блок: MLXB
x1(12)=12-5 mod 33 =7(K)
x2(11)=11-7 mod 33 =4(E)
x3(23)=23-2 mod 33 =21(V)
x4(23)=23-19 mod 33 =4(E)
Блок: JAEH
x1(9)=9-5 mod 33 =4(H)
x2(0)=0-7 mod 33 =19(T)
x3(4)=4-2 mod 33 =2(C)
x4(4)=4-19 mod 33 =11(L)
Блок: SNKG
x1(18)=18-5 mod 33 =13(Q)

x2(13)=13-7 mod 33 =6(G)
x3(10)=10-2 mod 33 =8(I)
x4(10)=10-19 mod 33 =17(R)
Блок: RVUV
x1(17)=17-5 mod 33 =12(P)
x2(21)=21-7 mod 33 =14(O)
x3(20)=20-2 mod 33 =18(S)
x4(20)=20-19 mod 33 =1(B)

Отже маємо дешифрований текст
ITWASDISCLOSEDYESTERDAYTHATSEVERALINFORMALBUTDIRECTCONTACTSHAVE
BEENMADEWITHPOLITICALREPRESENTIVESOFTHEVIETCONGINMOSCOW

Шифрування група 2

Маємо текст, який маємо зашифрувати

Зідентифікували ми тільки чотири літери, але маємо в розпорядженні не такий малий фрагмент відтвореного тексту. Продовження аналізу в такому напрямку шляхом проб і помилок приводить до повного відтворення відкритого тексту шифрограми.

Видаляємо пробіли і замінюємо всі символи на їх великі відповідники
ЗІДЕНТИФІКУВАЛИМИТІЛЬКИЧОТИРИЛІТЕРИАЛЕМАЄМОВРОЗПОРЯДЖЕННІНЕТАК
ИЙМАЛИЙФРАГМЕНТВІДТВОРЕНОГОТЕКСТУПРОДОВЖЕННЯАНАЛІЗУВТАКОМУНАП
РЯМКУШЛЯХОМПРОБІПОМИЛОКПРИВОДИТЬДОПОВНОГОВІДТВОРЕННЯВІДКРИТО
ГОТЕКСТУШИФРОГРАМИ
Вибермо параметри шифрування
$t = 3, j_1 = 2, j_2 = 5, j_3 = 12$
Блок: ЗІД
x1(9)=9+2 mod 33 =11(І)
x2(11)=11+5 mod 33 =16(М)
x3(5)=5+12 mod 33 =17(Н)
Блок: ЕНТ
x1(6)=6+2 mod 33 =8(Ж)
x2(17)=17+5 mod 33 =22(Т)
x3(22)=22+12 mod 33 =1(Б)
Блок: ИФІ
x1(10)=10+2 mod 33 =12(Ї)
x2(24)=24+5 mod 33 =29(Щ)
x3(11)=11+12 mod 33 =23(У)
Блок: КУВ
x1(14)=14+2 mod 33 =16(М)
x2(23)=23+5 mod 33 =28(Ш)
x3(2)=2+12 mod 33 =14(К)
Блок: АЛИ
x1(0)=0+2 mod 33 =2(В)
x2(15)=15+5 mod 33 =20(Р)

x3(10)=10+12 mod 33 =22(Т)
Блок: МИТ
x1(16)=16+2 mod 33 =18(О)
x2(10)=10+5 mod 33 =15(Л)
x3(22)=22+12 mod 33 =1(Б)
Блок: ІЛЬ
x1(11)=11+2 mod 33 =13(Й)
x2(15)=15+5 mod 33 =20(Р)
x3(30)=30+12 mod 33 =9(З)
Блок: КИЧ
x1(14)=14+2 mod 33 =16(М)
x2(10)=10+5 mod 33 =15(Л)
x3(27)=27+12 mod 33 =6(Е)
Блок: ОТИ
x1(18)=18+2 mod 33 =20(Р)
x2(22)=22+5 mod 33 =27(Ч)
x3(10)=10+12 mod 33 =22(Т)
Блок: РИЛ
x1(20)=20+2 mod 33 =22(Т)
x2(10)=10+5 mod 33 =15(Л)
x3(15)=15+12 mod 33 =27(Ч)
Блок: ІТЕ
x1(11)=11+2 mod 33 =13(Й)
x2(22)=22+5 mod 33 =27(Ч)
x3(6)=6+12 mod 33 =18(О)
Блок: РИА
x1(20)=20+2 mod 33 =22(Т)
x2(10)=10+5 mod 33 =15(Л)
x3(0)=0+12 mod 33 =12(Ї)
Блок: ЛЕМ
x1(15)=15+2 mod 33 =17(Н)
x2(6)=6+5 mod 33 =11(І)
x3(16)=16+12 mod 33 =28(Ш)
Блок: АЄМ
x1(0)=0+2 mod 33 =2(В)
x2(7)=7+5 mod 33 =12(Ї)
x3(16)=16+12 mod 33 =28(Ш)
Блок: ОВР
x1(18)=18+2 mod 33 =20(Р)
x2(2)=2+5 mod 33 =7(Є)
x3(20)=20+12 mod 33 =32(Я)
Блок: ОЗП
x1(18)=18+2 mod 33 =20(Р)
x2(9)=9+5 mod 33 =14(К)
x3(19)=19+12 mod 33 =31(Ю)
Блок: ОРЯ
x1(18)=18+2 mod 33 =20(Р)
x2(20)=20+5 mod 33 =25(Х)

x3(32)=32+12 mod 33 =11(І)
Блок: ДЖЕ
x1(5)=5+2 mod 33 =7(Є)
x2(8)=8+5 mod 33 =13(Й)
x3(6)=6+12 mod 33 =18(О)
Блок: ННІ
x1(17)=17+2 mod 33 =19(П)
x2(17)=17+5 mod 33 =22(Т)
x3(11)=11+12 mod 33 =23(У)
Блок: НЕТ
x1(17)=17+2 mod 33 =19(П)
x2(6)=6+5 mod 33 =11(І)
x3(22)=22+12 mod 33 =1(Б)
Блок: АКИ
x1(0)=0+2 mod 33 =2(В)
x2(14)=14+5 mod 33 =19(П)
x3(10)=10+12 mod 33 =22(Т)
Блок: ЙМА
x1(13)=13+2 mod 33 =15(Л)
x2(16)=16+5 mod 33 =21(С)
x3(0)=0+12 mod 33 =12(Ї)
Блок: ЛИЙ
x1(15)=15+2 mod 33 =17(Н)
x2(10)=10+5 mod 33 =15(Л)
x3(13)=13+12 mod 33 =25(Х)
Блок: ФРА
x1(24)=24+2 mod 33 =26(Ц)
x2(20)=20+5 mod 33 =25(Х)
x3(0)=0+12 mod 33 =12(Ї)
Блок: ГМЕ
x1(3)=3+2 mod 33 =5(Д)
x2(16)=16+5 mod 33 =21(С)
x3(6)=6+12 mod 33 =18(О)
Блок: НТВ
x1(17)=17+2 mod 33 =19(П)
x2(22)=22+5 mod 33 =27(Ч)
x3(2)=2+12 mod 33 =14(К)
Блок: ІДТ
x1(11)=11+2 mod 33 =13(Й)
x2(5)=5+5 mod 33 =10(И)
x3(22)=22+12 mod 33 =1(Б)
Блок: ВОР
x1(2)=2+2 mod 33 =4(Ґ)
x2(18)=18+5 mod 33 =23(У)
x3(20)=20+12 mod 33 =32(Я)
Блок: ЕНО
x1(6)=6+2 mod 33 =8(Ж)
x2(17)=17+5 mod 33 =22(Т)

x3(18)=18+12 mod 33 =30(Ь)
Блок: ГОТ
x1(3)=3+2 mod 33 =5(Д)
x2(18)=18+5 mod 33 =23(У)
x3(22)=22+12 mod 33 =1(Б)
Блок: ЕКС
x1(6)=6+2 mod 33 =8(Ж)
x2(14)=14+5 mod 33 =19(П)
x3(21)=21+12 mod 33 =0(А)
Блок: ТУП
x1(22)=22+2 mod 33 =24(Ф)
x2(23)=23+5 mod 33 =28(Ш)
x3(19)=19+12 mod 33 =31(Ю)
Блок: РОД
x1(20)=20+2 mod 33 =22(Т)
x2(18)=18+5 mod 33 =23(У)
x3(5)=5+12 mod 33 =17(Н)
Блок: ОВЖ
x1(18)=18+2 mod 33 =20(Р)
x2(2)=2+5 mod 33 =7(Є)
x3(8)=8+12 mod 33 =20(Р)
Блок: ЕНН
x1(6)=6+2 mod 33 =8(Ж)
x2(17)=17+5 mod 33 =22(Т)
x3(17)=17+12 mod 33 =29(Щ)
Блок: ЯАН
x1(32)=32+2 mod 33 =1(Б)
x2(0)=0+5 mod 33 =5(Д)
x3(17)=17+12 mod 33 =29(Щ)
Блок: АЛІ
x1(0)=0+2 mod 33 =2(В)
x2(15)=15+5 mod 33 =20(Р)
x3(11)=11+12 mod 33 =23(У)
Блок: ЗУВ
x1(9)=9+2 mod 33 =11(І)
x2(23)=23+5 mod 33 =28(Ш)
x3(2)=2+12 mod 33 =14(К)
Блок: ТАК
x1(22)=22+2 mod 33 =24(Ф)
x2(0)=0+5 mod 33 =5(Д)
x3(14)=14+12 mod 33 =26(Ц)
Блок: ОМУ
x1(18)=18+2 mod 33 =20(Р)
x2(16)=16+5 mod 33 =21(С)
x3(23)=23+12 mod 33 =2(В)
Блок: НАП
x1(17)=17+2 mod 33 =19(П)
x2(0)=0+5 mod 33 =5(Д)

x3(19)=19+12 mod 33 =31(Ю)
Блок: РЯМ
x1(20)=20+2 mod 33 =22(Т)
x2(32)=32+5 mod 33 =4(Ґ)
x3(16)=16+12 mod 33 =28(Ш)
Блок: КУШ
x1(14)=14+2 mod 33 =16(М)
x2(23)=23+5 mod 33 =28(Ш)
x3(28)=28+12 mod 33 =7(Є)
Блок: ЛЯХ
x1(15)=15+2 mod 33 =17(Н)
x2(32)=32+5 mod 33 =4(Ґ)
x3(25)=25+12 mod 33 =4(Ґ)
Блок: ОМП
x1(18)=18+2 mod 33 =20(Р)
x2(16)=16+5 mod 33 =21(С)
x3(19)=19+12 mod 33 =31(Ю)
Блок: РОБ
x1(20)=20+2 mod 33 =22(Т)
x2(18)=18+5 mod 33 =23(У)
x3(1)=1+12 mod 33 =13(Й)
Блок: ІПО
x1(11)=11+2 mod 33 =13(Й)
x2(19)=19+5 mod 33 =24(Ф)
x3(18)=18+12 mod 33 =30(Ь)
Блок: МИЛ
x1(16)=16+2 mod 33 =18(О)
x2(10)=10+5 mod 33 =15(Л)
x3(15)=15+12 mod 33 =27(Ч)
Блок: ОКП
x1(18)=18+2 mod 33 =20(Р)
x2(14)=14+5 mod 33 =19(П)
x3(19)=19+12 mod 33 =31(Ю)
Блок: РИВ
x1(20)=20+2 mod 33 =22(Т)
x2(10)=10+5 mod 33 =15(Л)
x3(2)=2+12 mod 33 =14(К)
Блок: ОДИ
x1(18)=18+2 mod 33 =20(Р)
x2(5)=5+5 mod 33 =10(И)
x3(10)=10+12 mod 33 =22(Т)
Блок: ТЬД
x1(22)=22+2 mod 33 =24(Ф)
x2(30)=30+5 mod 33 =2(В)
x3(5)=5+12 mod 33 =17(Н)
Блок: ОПО
x1(18)=18+2 mod 33 =20(Р)
x2(19)=19+5 mod 33 =24(Ф)

x3(18)=18+12 mod 33 =30(Ь)
Блок: ВНО
x1(2)=2+2 mod 33 =4(Ґ)
x2(17)=17+5 mod 33 =22(Т)
x3(18)=18+12 mod 33 =30(Ь)
Блок: ГОВ
x1(3)=3+2 mod 33 =5(Д)
x2(18)=18+5 mod 33 =23(У)
x3(2)=2+12 mod 33 =14(К)
Блок: ІДТ
x1(11)=11+2 mod 33 =13(Й)
x2(5)=5+5 mod 33 =10(И)
x3(22)=22+12 mod 33 =1(Б)
Блок: ВОР
x1(2)=2+2 mod 33 =4(Ґ)
x2(18)=18+5 mod 33 =23(У)
x3(20)=20+12 mod 33 =32(Я)
Блок: ЕНН
x1(6)=6+2 mod 33 =8(Ж)
x2(17)=17+5 mod 33 =22(Т)
x3(17)=17+12 mod 33 =29(Щ)
Блок: ЯВІ
x1(32)=32+2 mod 33 =1(Б)
x2(2)=2+5 mod 33 =7(Є)
x3(11)=11+12 mod 33 =23(У)
Блок: ДКР
x1(5)=5+2 mod 33 =7(Є)
x2(14)=14+5 mod 33 =19(П)
x3(20)=20+12 mod 33 =32(Я)
Блок: ИТО
x1(10)=10+2 mod 33 =12(Ї)
x2(22)=22+5 mod 33 =27(Ч)
x3(18)=18+12 mod 33 =30(Ь)
Блок: ГОТ
x1(3)=3+2 mod 33 =5(Д)
x2(18)=18+5 mod 33 =23(У)
x3(22)=22+12 mod 33 =1(Б)
Блок: ЕКС
x1(6)=6+2 mod 33 =8(Ж)
x2(14)=14+5 mod 33 =19(П)
x3(21)=21+12 mod 33 =0(А)
Блок: ТУШ
x1(22)=22+2 mod 33 =24(Ф)
x2(23)=23+5 mod 33 =28(Ш)
x3(28)=28+12 mod 33 =7(Є)
Блок: ИФР
x1(10)=10+2 mod 33 =12(Ї)
x2(24)=24+5 mod 33 =29(Щ)

x3(20)=20+12 mod 33 =32(Я)
Блок: ОГР
x1(18)=18+2 mod 33 =20(Р)
x2(3)=3+5 mod 33 =8(Ж)
x3(20)=20+12 mod 33 =32(Я)
Блок: АМИ
x1(0)=0+2 mod 33 =2(В)
x2(16)=16+5 mod 33 =21(С)
x3(10)=10+12 mod 33 =22(Т)

Отже зашифрований текст має вигляд

ІМН ЖТБ ЇЩУ МШК ВРТ ОЛБ ЙРЗ МЛЕ РЧТ ТЛЧ ЙЧО ТЛЇ НІШ ВЇШ РЄЯ РКЮ РХІ ЄЙО ПТУ ПІБ ВПТ ЛСЇ НЛХ ЦХЇ ДСО ПЧК ЙИБ ҐУЯ ЖТЬ ДУБ ЖПА ФШЮ ТУН РЄР ЖТЩ БДЩ ВРУ ІШК ФДЦ РСВ ПДЮ ТҐШ МШЄ НҐҐ РСЮ ТУЙ ЙФЬ ОЛЧ РПЮ ТЛК РИТ ФВН РФЬ ҐТЬ ДУК ЙИБ ҐУЯ ЖТЩ БЄУ ЄПЯ ЇЧЬ ДУБ ЖПА ФШЄ ЇЩЯ РЖЯ ВСТ

Дешифрування група 1

Маємо вхідні параметри $t = 3$, $j_1 = 2$, $j_2 = 5$, $j_3 = 12$

Та вхідний шифротекст
ІМН ЖТБ ЇЩУ МШК ВРТ ОЛБ ЙРЗ МЛЕ РЧТ ТЛЧ ЙЧО ТЛЇ НІШ ВЇШ РЄЯ РКЮ РХІ ЄЙО ПТУ ПІБ ВПТ ЛСЇ НЛХ ЦХЇ ДСО ПЧК ЙИБ ҐУЯ ЖТЬ ДУБ ЖПА ФШЮ ТУН РЄР ЖТЩ БДЩ ВРУ ІШК ФДЦ РСВ ПДЮ ТҐШ МШЄ НҐҐ РСЮ ТУЙ ЙФЬ ОЛЧ РПЮ ТЛК РИТ ФВН РФЬ ҐТЬ ДУК ЙИБ ҐУЯ ЖТЩ БЄУ ЄПЯ ЇЧЬ ДУБ ЖПА ФШЄ ЇЩЯ РЖЯ ВСТ

Обернені функції підстановок:

$x_1^{-1}(k) = (k - j_1) \, mod \, 33$

$x_2^{-1}(k) = (k - j_2) \, mod \, 33$

$x_3^{-1}(k) = (k - j_3) \, mod \, 33$

Блок: ІМН
x1(11)=11-2 mod 33 =9(З)
x2(16)=16-5 mod 33 =11(І)
x3(17)=17-12 mod 33 =5(Д)
Блок: ЖТБ
x1(8)=8-2 mod 33 =6(Е)
x2(22)=22-5 mod 33 =17(Н)
x3(1)=1-12 mod 33 =22(Т)
Блок: ЇЩУ
x1(12)=12-2 mod 33 =10(И)
x2(29)=29-5 mod 33 =24(Ф)

x3(23)=23-12 mod 33 =11(І)
Блок: МШК
x1(16)=16-2 mod 33 =14(К)
x2(28)=28-5 mod 33 =23(У)
x3(14)=14-12 mod 33 =2(В)
Блок: ВРТ
x1(2)=2-2 mod 33 =0(А)
x2(20)=20-5 mod 33 =15(Л)
x3(22)=22-12 mod 33 =10(И)
Блок: ОЛБ
x1(18)=18-2 mod 33 =16(М)
x2(15)=15-5 mod 33 =10(И)
x3(1)=1-12 mod 33 =22(Т)
Блок: ЙРЗ
x1(13)=13-2 mod 33 =11(І)
x2(20)=20-5 mod 33 =15(Л)
x3(9)=9-12 mod 33 =30(Ь)
Блок: МЛЕ
x1(16)=16-2 mod 33 =14(К)
x2(15)=15-5 mod 33 =10(И)
x3(6)=6-12 mod 33 =27(Ч)
Блок: РЧТ
x1(20)=20-2 mod 33 =18(О)
x2(27)=27-5 mod 33 =22(Т)
x3(22)=22-12 mod 33 =10(И)
Блок: ТЛЧ
x1(22)=22-2 mod 33 =20(Р)
x2(15)=15-5 mod 33 =10(И)
x3(27)=27-12 mod 33 =15(Л)
Блок: ЙЧО
x1(13)=13-2 mod 33 =11(І)
x2(27)=27-5 mod 33 =22(Т)
x3(18)=18-12 mod 33 =6(Е)
Блок: ТЛЇ
x1(22)=22-2 mod 33 =20(Р)
x2(15)=15-5 mod 33 =10(И)
x3(12)=12-12 mod 33 =0(А)
Блок: НІШ
x1(17)=17-2 mod 33 =15(Л)
x2(11)=11-5 mod 33 =6(Е)
x3(28)=28-12 mod 33 =16(М)
Блок: ВЇШ
x1(2)=2-2 mod 33 =0(А)
x2(12)=12-5 mod 33 =7(Є)
x3(28)=28-12 mod 33 =16(М)
Блок: РЄЯ
x1(20)=20-2 mod 33 =18(О)
x2(7)=7-5 mod 33 =2(В)

x3(32)=32-12 mod 33 =20(Р)
Блок: РКЮ
x1(20)=20-2 mod 33 =18(О)
x2(14)=14-5 mod 33 =9(З)
x3(31)=31-12 mod 33 =19(П)
Блок: РХІ
x1(20)=20-2 mod 33 =18(О)
x2(25)=25-5 mod 33 =20(Р)
x3(11)=11-12 mod 33 =32(Я)
Блок: ЄЙО
x1(7)=7-2 mod 33 =5(Д)
x2(13)=13-5 mod 33 =8(Ж)
x3(18)=18-12 mod 33 =6(Е)
Блок: ПТУ
x1(19)=19-2 mod 33 =17(Н)
x2(22)=22-5 mod 33 =17(Н)
x3(23)=23-12 mod 33 =11(І)
Блок: ПІБ
x1(19)=19-2 mod 33 =17(Н)
x2(11)=11-5 mod 33 =6(Е)
x3(1)=1-12 mod 33 =22(Т)
Блок: ВПТ
x1(2)=2-2 mod 33 =0(А)
x2(19)=19-5 mod 33 =14(К)
x3(22)=22-12 mod 33 =10(И)
Блок: ЛСЇ
x1(15)=15-2 mod 33 =13(Й)
x2(21)=21-5 mod 33 =16(М)
x3(12)=12-12 mod 33 =0(А)
Блок: НЛХ
x1(17)=17-2 mod 33 =15(Л)
x2(15)=15-5 mod 33 =10(И)
x3(25)=25-12 mod 33 =13(Й)
Блок: ЦХЇ
x1(26)=26-2 mod 33 =24(Ф)
x2(25)=25-5 mod 33 =20(Р)
x3(12)=12-12 mod 33 =0(А)
Блок: ДСО
x1(5)=5-2 mod 33 =3(Г)
x2(21)=21-5 mod 33 =16(М)
x3(18)=18-12 mod 33 =6(Е)
Блок: ПЧК
x1(19)=19-2 mod 33 =17(Н)
x2(27)=27-5 mod 33 =22(Т)
x3(14)=14-12 mod 33 =2(В)
Блок: ЙИБ
x1(13)=13-2 mod 33 =11(І)
x2(10)=10-5 mod 33 =5(Д)

x3(1)=1-12 mod 33 =22(Т)
Блок: ҐУЯ
x1(4)=4-2 mod 33 =2(В)
x2(23)=23-5 mod 33 =18(О)
x3(32)=32-12 mod 33 =20(Р)
Блок: ЖТЬ
x1(8)=8-2 mod 33 =6(Е)
x2(22)=22-5 mod 33 =17(Н)
x3(30)=30-12 mod 33 =18(О)
Блок: ДУБ
x1(5)=5-2 mod 33 =3(Г)
x2(23)=23-5 mod 33 =18(О)
x3(1)=1-12 mod 33 =22(Т)
Блок: ЖПА
x1(8)=8-2 mod 33 =6(Е)
x2(19)=19-5 mod 33 =14(К)
x3(0)=0-12 mod 33 =21(С)
Блок: ФШЮ
x1(24)=24-2 mod 33 =22(Т)
x2(28)=28-5 mod 33 =23(У)
x3(31)=31-12 mod 33 =19(П)
Блок: ТУН
x1(22)=22-2 mod 33 =20(Р)
x2(23)=23-5 mod 33 =18(О)
x3(17)=17-12 mod 33 =5(Д)
Блок: РЄР
x1(20)=20-2 mod 33 =18(О)
x2(7)=7-5 mod 33 =2(В)
x3(20)=20-12 mod 33 =8(Ж)
Блок: ЖТЩ
x1(8)=8-2 mod 33 =6(Е)
x2(22)=22-5 mod 33 =17(Н)
x3(29)=29-12 mod 33 =17(Н)
Блок: БДЩ
x1(1)=1-2 mod 33 =32(Я)
x2(5)=5-5 mod 33 =0(А)
x3(29)=29-12 mod 33 =17(Н)
Блок: ВРУ
x1(2)=2-2 mod 33 =0(А)
x2(20)=20-5 mod 33 =15(Л)
x3(23)=23-12 mod 33 =11(І)
Блок: ІШК
x1(11)=11-2 mod 33 =9(З)
x2(28)=28-5 mod 33 =23(У)
x3(14)=14-12 mod 33 =2(В)
Блок: ФДЦ
x1(24)=24-2 mod 33 =22(Т)
x2(5)=5-5 mod 33 =0(А)

x3(26)=26-12 mod 33 =14(К)
Блок: РСВ
x1(20)=20-2 mod 33 =18(О)
x2(21)=21-5 mod 33 =16(М)
x3(2)=2-12 mod 33 =23(У)
Блок: ПДЮ
x1(19)=19-2 mod 33 =17(Н)
x2(5)=5-5 mod 33 =0(А)
x3(31)=31-12 mod 33 =19(П)
Блок: ТҐШ
x1(22)=22-2 mod 33 =20(Р)
x2(4)=4-5 mod 33 =32(Я)
x3(28)=28-12 mod 33 =16(М)
Блок: МШЄ
x1(16)=16-2 mod 33 =14(К)
x2(28)=28-5 mod 33 =23(У)
x3(7)=7-12 mod 33 =28(Ш)
Блок: НҐҐ
x1(17)=17-2 mod 33 =15(Л)
x2(4)=4-5 mod 33 =32(Я)
x3(4)=4-12 mod 33 =25(Х)
Блок: РСЮ
x1(20)=20-2 mod 33 =18(О)
x2(21)=21-5 mod 33 =16(М)
x3(31)=31-12 mod 33 =19(П)
Блок: ТУЙ
x1(22)=22-2 mod 33 =20(Р)
x2(23)=23-5 mod 33 =18(О)
x3(13)=13-12 mod 33 =1(Б)
Блок: ЙФЬ
x1(13)=13-2 mod 33 =11(І)
x2(24)=24-5 mod 33 =19(П)
x3(30)=30-12 mod 33 =18(О)
Блок: ОЛЧ
x1(18)=18-2 mod 33 =16(М)
x2(15)=15-5 mod 33 =10(И)
x3(27)=27-12 mod 33 =15(Л)
Блок: РПЮ
x1(20)=20-2 mod 33 =18(О)
x2(19)=19-5 mod 33 =14(К)
x3(31)=31-12 mod 33 =19(П)
Блок: ТЛК
x1(22)=22-2 mod 33 =20(Р)
x2(15)=15-5 mod 33 =10(И)
x3(14)=14-12 mod 33 =2(В)
Блок: РИТ
x1(20)=20-2 mod 33 =18(О)
x2(10)=10-5 mod 33 =5(Д)

x3(22)=22-12 mod 33 =10(И)
Блок: ФВН
x1(24)=24-2 mod 33 =22(Т)
x2(2)=2-5 mod 33 =30(Ь)
x3(17)=17-12 mod 33 =5(Д)
Блок: РФЬ
x1(20)=20-2 mod 33 =18(О)
x2(24)=24-5 mod 33 =19(П)
x3(30)=30-12 mod 33 =18(О)
Блок: ҐТЬ
x1(4)=4-2 mod 33 =2(В)
x2(22)=22-5 mod 33 =17(Н)
x3(30)=30-12 mod 33 =18(О)
Блок: ДУК
x1(5)=5-2 mod 33 =3(Г)
x2(23)=23-5 mod 33 =18(О)
x3(14)=14-12 mod 33 =2(В)
Блок: ЙИБ
x1(13)=13-2 mod 33 =11(І)
x2(10)=10-5 mod 33 =5(Д)
x3(1)=1-12 mod 33 =22(Т)
Блок: ҐУЯ
x1(4)=4-2 mod 33 =2(В)
x2(23)=23-5 mod 33 =18(О)
x3(32)=32-12 mod 33 =20(Р)
Блок: ЖТЩ
x1(8)=8-2 mod 33 =6(Е)
x2(22)=22-5 mod 33 =17(Н)
x3(29)=29-12 mod 33 =17(Н)
Блок: БЄУ
x1(1)=1-2 mod 33 =32(Я)
x2(7)=7-5 mod 33 =2(В)
x3(23)=23-12 mod 33 =11(І)
Блок: ЄПЯ
x1(7)=7-2 mod 33 =5(Д)
x2(19)=19-5 mod 33 =14(К)
x3(32)=32-12 mod 33 =20(Р)
Блок: ЇЧЬ
x1(12)=12-2 mod 33 =10(И)
x2(27)=27-5 mod 33 =22(Т)
x3(30)=30-12 mod 33 =18(О)
Блок: ДУБ
x1(5)=5-2 mod 33 =3(Г)
x2(23)=23-5 mod 33 =18(О)
x3(1)=1-12 mod 33 =22(Т)
Блок: ЖПА
x1(8)=8-2 mod 33 =6(Е)
x2(19)=19-5 mod 33 =14(К)

x3(0)=0-12 mod 33 =21(С)
Блок: ФШЄ
x1(24)=24-2 mod 33 =22(Т)
x2(28)=28-5 mod 33 =23(У)
x3(7)=7-12 mod 33 =28(Ш)
Блок: ЇЩЯ
x1(12)=12-2 mod 33 =10(И)
x2(29)=29-5 mod 33 =24(Ф)
x3(32)=32-12 mod 33 =20(Р)
Блок: РЖЯ
x1(20)=20-2 mod 33 =18(О)
x2(8)=8-5 mod 33 =3(Г)
x3(32)=32-12 mod 33 =20(Р)
Блок: ВСТ
x1(2)=2-2 mod 33 =0(А)
x2(21)=21-5 mod 33 =16(М)
x3(22)=22-12 mod 33 =10(И)

Отже маємо дешифрований текст:

ЗІДЕНТИФІКУВАЛИМИТІЛЬКИЧОТИРИЛІТЕРИАЛЕМАЄМОВРОЗПОРЯДЖЕННІНЕТАК
ИЙМАЛИЙФРАГМЕНТВІДТВОРЕНОГОТЕКСТУПРОДОВЖЕННЯАНАЛІЗУВТАКОМУНАП
РЯМКУШЛЯХОМПРОБІПОМИЛОКПРИВОДИТЬДОПОВНОГОВІДТВОРЕННЯВІДКРИТО
ГОТЕКСТУШИФРОГРАМИ

Література

- Лекції з предмету “Математичні основи захисту інформації”
- https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9_%D1%88%D0%B8%D1%84%D1%80
- https://www.wikiwand.com/uk/%D0%91%D0%BB%D0%BE%D0%BA%D0%BE%D0%B2%D0%B8%D0%B9_%D1%88%D0%B8%D1%84%D1%80