Криптографические методы защиты информации

Практическая работа № 1

Блочное симметричное шифрование

Цель работы

Практическое изучение особенностей работы одного из методов построения блочных шифров – сети Фейстеля.

Форма контроля

Опрос в устной форме по исходному коду и результатам работы реализованной программы

Количество отведённых аудиторных часов

10

Содержание работы

Получить у преподавателя вариант задания, написать код, реализующий соответствующий алгоритм обработки информации. Провести тестирование реализованного алгоритма при различных значениях параметров. Проанализировать полученные результаты и сформулировать выводы по проделанной работе.

Пример варианта задания:

Реализовать процедуры шифрования и расшифровки информации с использованием сети Фейстеля заданной архитектуры (рисунок 1). Размер шифруемого блока 64 бита (*b*=6), размеры подблоков L и R по 32 бита. Секретный ключ K – случайная 64-битная последовательность. Раундовые ключи $K_i = (K >>> i*8)_{0..31}$, $i = \overline{0, n-1}$. Число раундов n изменяется от 2 до 12. Образующая функция $F(L_i, K_i) = (L_i <<< 9) \oplus (\sim ((K_i >>> 11) \otimes L_i))$, $i = \overline{0, n-1}$. Исследовать влияние параметров сети на качество получаемых зашифрованных последовательностей.

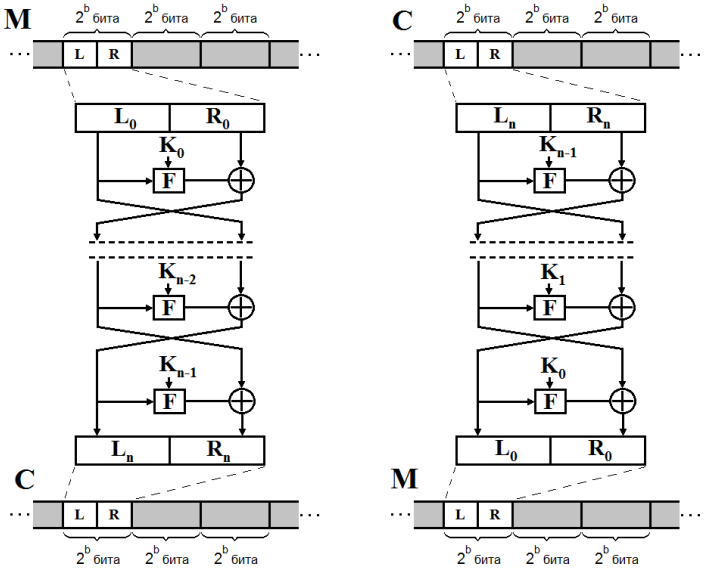

Рисунок 1

Примеры контрольных вопросов:

1. На примере своего варианта реализации практического задания пояснить свойства симметричности и обратимости сети Фейстеля.

2. Каким способом достигаются эффекты рассеивания и перемешивания?

Криптографические методы защиты информации

Практическая работа № 2

Изучение режимов работы блочных симметричных алгоритмов шифрования данных

Цель работы

Изучение режимов работы блочных симметричных алгоритмов шифрования данных.

Форма контроля

Опрос в устной форме по исходному коду и результатам работы реализованной программы

Количество отведённых аудиторных часов

8

Содержание работы

Получить у преподавателя вариант задания, написать код, реализующий соответствующий алгоритм обработки информации. Провести тестирование реализованного алгоритма. Проанализировать полученные результаты и сформулировать выводы по проделанной работе.

Пример варианта задания:

Модифицировать реализованный в практической работе №1 вариант блочного шифрования на основе сети Фейстеля для работы в режимах CBC (Cipher Block Chaining) и CFB (Cipher Feedback).

Примеры контрольных вопросов:

1. Какие требования предъявляются к генерации и хранению вектора инициализации в режимах шифрования CBC и CFB?
2. В каких практических приложениях целесообразно и не целесообразно использовать каждый из режимов шифрования: ECB (Electronic Codebook), CBC, CFB, OFB (Output Feedback), CTR(Counter)?

Криптографические методы защиты информации

Практическая работа № 3

Изучение работы генераторов последовательностей

псевдослучайных чисел

L:\лекции\4 курс\Инф. Безопасность\Лаборатория ЗИ\s084.pdf

Цель работы

Изучение работы алгоритмов генерации последовательностей псевдослучайных чисел.

Форма контроля

Опрос в устной форме по исходному коду и результатам работы реализованной программы.

Количество отведённых аудиторных часов

8

Содержание работы

Получить у преподавателя вариант задания, написать код, реализующий соответствующий алгоритм обработки информации. Провести тестирование реализованного алгоритма. Проанализировать полученные результаты и сформулировать выводы по проделанной работе.

Пример варианта задания:

Реализовать Линейный конгруэнтный генератор Лемера

$$U_{i+1} = (U_i * M + C) \bmod p,$$

где U_i, M, C и p – целые числа. Исследовать при каких U_0, p и M длина последовательности неповторяющихся чисел будет не менее 10000 при «хороших» стохастических параметрах. Определить влияет ли величина R_0 при M и $p=const$ на статистические характеристики алгоритма. Если влияет, то определить область допустимых величин U_0. Представить результаты тестирования генератора для оптимальных величин p, M и U_0.

Примеры контрольных вопросов:

1. Какие требования предъявляются к криптографически стойким генераторам псевдослучайных последовательностей?
2. Как определить длину периода псевдослучайной числовой последовательности?

Криптографические методы защиты информации

Практическая работа № 4

Изучение работы асимметричных алгоритмов шифрования

Цель работы

Изучение работы асимметричных алгоритмов шифрования на примере алгоритма RSA.

Форма контроля

Опрос в устной форме по исходному коду и результатам работы реализованной программы.

Количество отведённых аудиторных часов

8

Содержание работы

Получить у преподавателя вариант задания, написать код, реализующий соответствующий алгоритм обработки информации. Провести тестирование реализованного алгоритма. Проанализировать полученные результаты и сформулировать выводы по проделанной работе.

Пример варианта задания:

Провести дешифрование текста, зашифрованного алгоритмом RSA, на основе известного открытого ключа K_p и шифрованного текста C.

$$K_p = \{n=471090785117207;\ e=12377\}$$

$$C = 31499911228106520536170634151732198749109866 7$$

Примеры контрольных вопросов:

1. На чем основывается надежность алгоритма RSA?
2. Какие преобразования лежат в основе криптосистем с открытым ключом?

Криптографические методы защиты информации

Практическая работа № 5

Изучение частотного метода криптоанализа симметричных криптосистем

Цель работы

Практическое изучение частотного метода криптоанализа на примере криптосистемы Цезаря.

Форма контроля

Опрос в устной форме по исходному коду и результатам работы реализованной программы.

Количество отведённых аудиторных часов

6

Содержание работы

Получить у преподавателя вариант задания, написать код, реализующий соответствующий алгоритм обработки информации. Провести тестирование реализованного алгоритма. Проанализировать полученные результаты и сформулировать выводы по проделанной работе.

Пример варианта задания:

Используя метод частотного анализа и типовые таблицы частот встречаемости букв русского и английского алфавита дешифровать заданные криптограммы:

С1 = {щ зсдлъэд фцяб цоцюъбк сня пбь емйюсцдъ й цяъцк йюцсцъб йюмсэъъбжэ яцжмжэ, м й ясыфцк - яьэъъбж цяъцгюмлъбж еямъэдж зця цяъцк исбудк, ъдйжцюсн ъм юц, аюц цъц зсэъмяьдлмьц ядйнюимж щьмядьчшдщ. эе щйдо гюэо еямъэк юцьчиц ящм яцжм пбьэ лэьбжэ: яцж, фяд фцйюэъэшм "ицъюэъдъюмьч", ям йюцнвэк сняцж й ъэж юсмиюэс дфцсцщм, еъмждъэюбк йщцэжэ пьэъмжэ. цйюмьчъцд щйд ьмщиэ, щзьцюч яц ющдсйицк.

юсмиюэс дфцсцщм ицфям-юц зсэъмяьдлмь щцсцъэъы, э ъм щбщдйид пбьм эецпсмлдъм щцсцъм, ядслмвмн щ иьтщд пьэъ. щйд ьмщиэ цоцюъцфц сням пбьэ жнйъбд, сбпъбд, м зця ъэжэ едьдъъбд зцящмьб. емяъэд ящдсэ ьмщци щбоцяэьэ ъм цфсцжъбк ящцс-жцъдюъбк, ими дфц ъмебщмьэ эеясдщьд. ъм ъдж пбьэ юцлд цяъцгюмлъбд жнйъбд, лэщцсбпъбд э нэаъбд ьмщиэ, м зцйсдяэъд--ящыогюмлъбк "жцъдюъбк" юсмиюэс. щ емяъдк амйюэ ящцсм - сня ймсмтуди й зцфсдпмжэ э иьмяцщбжэ, иэудщуэжэ зцьаэвмжэ исбй.

цоцюъбк сня зцыыаэь йщцд ъмещмъэд двд щ юд щсджъдъм, ицфям еядйч смесдудъц пбьц юцсфцщмюч яэачт, зсэъцйэжцк зцяжцйицщъбжэ цоцюъэимжэ.

щздсдяэ ьмщци, ъм зьцвмяэ, щяцьч уэсцицфц юсцюымсм, йюцньэ здсдъцйъбд змьмюиэ э юцьзэьэйч юцсфцщшб й ицсеэъмжэ э ждуимжэ, ъмзцьъдъъбжэ щйдщцежцлъбжэ зсцяыиюмжэ. оцяэьэ цоцюъэиэ, цпшдумъъбд ыюимжэ, юдюдсимжэ, емкшмжэ. ы пмп эе ицсеэъ юцсамьэ фцьцщб иыс э шбзьню, щ ждуимо щэелмьэ зцсцйнюм, ицюцсбо зсцямщшб, щбъэжмн эе ждуим,аюцпб зцимемюч зциызмюдьт, ъдзсджъъц зцяъэжмьэ ъмя фцьцщцк, ядслм ем йщнемъъбд емяъэд ъцфэ. ъм жцйюцщцк здсдя змьмюимжэ йъцщмьэ зэсцлъэиэ, пьэъъэиэ, юцсфцщшб фсдаъдщэимжэ, лмсдъъбжэ ъм зцйюъцж жмйьд. йпэюдъвэиэ смеьэщмьэ, зц ицздкид ем йюмимъ, фцснаэк йпэюдъч - ьтпэжбк юцфям ждяцщбк

ъмзэюци, йцфсдщмщуэк эещцеаэицщ э йьылмвэо, емждсемщуэо щ оцьцяъбо ьмщимо. ьдюцж йпэюдъвэицщ йждъньэ юцсфцщшб ищмймжэ, э ймжбк ьтпэжбк эе ъэо пбь фсыудщбк, эе щмсдъбо фсыу, ицюцсбд щ жцадъцж щэяд ьдлмьэ яьн зсцямлэ зэсмжэямжэ ъм ьцюимо, м ищмй адсзмьэ эе щдясм исылимжэ. жнйъбд э сбпъбд ьмщиэ йцйюцньэ эе ящыо цюядьдъэк. щ здсщцж ьдлмьц ъм зцьимо жнйц смеъбо йцсюцщ - яэач, иысб, фыйэ, эъядкиэ, змьдъбд зцсцйнюм яьн лмсицфц э щ ьдянъбо щмъъмо - пдьбд зцсцйнюм яьн емьэщъцфц. ъм истачно зц йюдъмж пбьэ смещдумъб юыуэ пмсмуицщ э зцдъъбо жцьцицж юдьню, м щдйч зцюцьци емъню цицсцимжэ щйдщцежцлъбо смеждсцщ э зсэфцюцщьдъэк--ицзадъбо, щмсдъбо, зсцщдйъбо. щц щюцсцж цюядьдъээ, юджъцж, цйщдвдъъцж юцьчиц ящдсчт щц ящцс, щэйдьэ ядйнюиэ жнйъбо юыу. зця щйджэ ьмщимжэ -- зцящмьб. цоцюъбк сня пбщмь цйцпдъъц цлэщьдъъбж здсдя пцьчуэжэ

зсмеяъэимжэ. и ьмщимж зцяхделмьэ ъм юбйнаъбо сбймимо смйрсмъадъъбд иызаэоэ, э ем ъэжэ йьылмвэд щбъцйэьэ эе ьмщци}

C2 = { pyt viqebov, xp q bqcvmc oxgvmzv jylof myc bvtexc tyrqocr-ptvv tvfxzctxhlcxym yp cwv btystqe hr qoo cwyzv jwy tvgvxnv gybxvz fxtvgcor yt xmfxtvgcor cwtylsw ryl, cwvm cwv ymor jqr ryl gylof zqcxzpr hycw xc qmf cwxz oxgvmzv jylof hv cy tvptqxm vmcxtvor ptye fxzctxhlcxym yp cwv btystqe.
xp qmr bytcxym yp cwxz zvgcxym xz wvof xmnqoxf yt lmvmpytgvqhov lmfvt qmr bqtcxgloqt gxtglezcqmgv, cwv hqoqmgv yp cwv zvgcxym xz xmcvmfvf cy qbbor qmf cwv zvgcxym qz q jwyov xz xmcvmfvf cy qbbor xm ycwvt gxtglezcqmgvz.
xc xz myc cwv bltbyzv yp cwxz zvgcxym cy xmflgv ryl cy xmptxmsv qmr bqcvmcz yt ycwvt btybvtcr txswc goqxez yt cy gymcvzc nqoxfxcr yp qmr zlgw goqxez; cwxz zvgcxym wqz cwv zyov bltbyzv yp btycvgcxms cwv xmcvstxcr yp cwv ptvv zypcjqtv fxzctxhlcxym zrzcve, jwxgw xz xebovevmcvf hr blhoxg oxgvmzv btqgcxgvz. eqmr bvybov wqnv eqfv svmvtylz gymctxhlcxymz cy cwv jxfv tqmsv yp zypcjqtv fxzctxhlcvf
cwtylsw cwqc zrzcve xm tvoxqmgv ym gymzxzcvmc qbboxgqcxym yp cwqc zrzcve; xc xz lb cy cwv qlcwyt/fymyt cy fvgxfv xp wv yt zwv xz jxooxms cy fxzctxhlcv zypcjqtv cwtylsw qmr ycwvt zrzcve qmf q oxgvmzvv gqmmyc xebyzv cwqc gwyxgv.
cwxz zvgcxym xz xmcvmfvf cy eqdv cwytylswor govqt jwqc xz hvoxvnvf cy hv q gymzvalvmgv yp cwv tvzc yp cwxz oxgvmzv.
xp cwv fxzctxhlcxym qmf/yt lzv yp cwv btystqe xz tvzctxgcvf xm gvtcqxm gylmctxvz vxcwvt hr bqcvmcz yt hr gybrtxswcvf xmcvtpqgvz, cwv ytxsxmqo gybrtxswc wyofvt jwy boqgvz cwv btystqe lmfvt cwxz oxgvmzv eqr qff qm viboxgxc svystqbwxgqo fxzctxhlcxym oxexcqcxym vigolfxms cwyzv gylmctxvz, zy cwqc fxzctxhlcxym xz bvtexccvf ymor xm yt qeyms gylmctxvz myc cwlz vigolfvf. xm zlgw gqzv, cwxz oxgvmzv xmgytbytqcvz cwv oxexcqcxym qz xp jtxccvm xm cwv hyfr yp cwxz oxgvmzv.
cwv ptvv zypcjqtv pylmfqcxym eqr blhoxzw tvnxzvf qmf/yt mvj nvtzxymz yp cwv svmvtqo blhoxg oxgvmzv ptye cxev cy cxev. zlgw mvj nvtzxymz jxoo hv zxexoqt xm zbxtxc cy cwv btvzvmc nvtzxym, hlc eqr fxppvt xm fvcqxo cy qfftvzz mvj btyhovez yt gymgvtmz.
vqgw nvtzxym xz sxnvm q fxzcxmslxzwxms nvtzxym mlehvt. xp cwv btystqe zbvgxpxvz q nvtzxym mlehvt yp cwxz oxgvmzv jwxgw qbboxvz cy xc qmf "qmr oqcvt nvtzxym", ryl wqnv cwv ybcxym yp pyooyjxms cwv cvtez qmf gymfxcxymz vxcwvt yp cwqc nvtzxym yt yp qmr oqcvt nvtzxym blhoxzwvf hr cwv ptvv
zypcjqtv pylmfqcxym. xp cwv btystqe fyvz myc zbvgxpr q nvtzxym mlehvt yp cwxz oxgvmzv, ryl eqr gwyyzv qmr nvtzxym vnvt blhoxzwvf hr cwv ptvv zypcjqtv pylmfqcxym.
xp ryl jxzw cy xmgytbytqcv bqtcz yp cwv btystqe xmcy ycwvt ptvv btystqez jwyzv fxzctxhlcxym gymfxcxymz qtv fxppvtvmc, jtxcv cy cwv qlcwyt cy qzd pyt bvtexzzxym. pyt zypcjqtv jwxgw xz gybrtxswcvf hr cwv ptvv zypcjqtv pylmfqcxym, jtxcv cy cwv ptvv zypcjqtv pylmfqcxym; jv zyevcxevz
eqdv vigvbcxymz pyt cwxz. ylt fvgxzxym jxoo hv slxfvf hr cwv cjy syqoz yp btvzvtnxms cwv ptvv zcqclz yp qoo fvtxnqcxnvz yp ylt ptvv zypcjqtv qmf yp btyeycxms cwv zwqtxms qmf tvlzv yp zypcjqtv svmvtqoor.
hvgqlzv cwv btystqe xz oxgvmzvf ptvv yp gwqtsv, cwvtv xz my jqttqmcr pyt cwv btystqe, cy cwv vicvmc bvtexccvf hr qbboxgqhov oqj. vigvbc jwvm ycwvtjxzv zcqcvf xm jtxcxms cwv gybrtxswc wyofvtz qmf/yt ycwvt bqtcxvz btynxfv cwv btystqe "qz xz" jxcwylc jqttqmcr yp qmr dxmf, vxcwvt vibtvzzvf
yt xeboxvf, xmgolfxms, hlc myc oxexcvf cy, cwv xeboxvf jqttqmcxvz yp evtgwqmcqhxoxcr qmf pxcmvzz pyt q bqtcxgloqt bltbyzv. cwv vmcxtv txzd qz cy cwv alqoxcr qmf bvtpyteqmgv yp cwv btystqe xz jxcw ryl. zwylof cwv btystqe btynv fvpvgcxnv, ryl qzzlev cwv gyzc yp qoo mvgvzzqtr zvtnxgxms, tvbqxt yt gyttvgcxym }

Примеры контрольных вопросов:

1. Таблица Виженера и полиалфавитные шифры.
2. Дифференциальный криптоанализ.