Криптография

Кевролетин В.В.

12 декабря 2011 г.

Задание 1.1

Условие

Сколько возможных ключей позволяет использовать шифр Плейфейра? (Представить в виде степени двойки.)

Решение

Если не ограничиваться представлением ключа в виде таблицы 5x5, то существует C_{25}^2 пар букв для алфавита из 25ти символов. Тогда существует $C_{25}^2!$ способов поставить в соответсвие одной паре другую.

Если же рассматривать только способ задания ключа в виде квадратной таблицы, то существует 25! способов заполнить квадратную таблицу символами (для алфавита из 25ти символов). При этом если производить циклический сдвиг строк или столбцов ключ не изменится, поэтому чтобы избавиться от разных записей одного и того же ключа необходимо разделить на поличество строк и столбцов. В итоге получаем $\frac{25!}{5*5}$ различных ключей.

Задание 1.2

Условие

Реализовать (Mathematica, Scheme, Sage, ...) схему шифрования-дешифрования Плейфейера, подготовить тесты по методу белого ящика, продемонстрировать его работу и методику криптоанализа на достаточно длинном шифрованном тексте.

Решение

Язык реализации: Перл

```
use warnings;
use strict;

sub split_to_pairs {
    my ($t) = @_;
    my @res;
    my $last = '';
```

```
    for (split //, $t) {
        if ($last) {
            push @res, [$last, $_];
            $last = undef;
        } else {
            $last = $_
        }
    }
    @res
}

sub table {
    my ($key) = @_;
    my %used = ('J' => 1);
    my ($t, $h);
    my $i = 0;
    for ((split //, $key), 'A' .. 'Z') {
        next if $used{$_};
        $t->[$i / 5][$i % 5] = $_;
        $h->{$_} = {x => $i % 5, y => int $i / 5};
        $used{$_} = 1;
        ++$i;
    }
    { table => $t, coords => $h}
}

sub encode_pair {
    my ($t, $pair) = @_;
    my ($a, $b) = (map { $t->{coords}->{$_} } @$pair);
    if ($a->{x} == $b->{x}) {
        $t->{table}->[$a->{y}][($a->{x} + 1) % 5] .
        $t->{table}->[$b->{y}][($b->{x} + 1) % 5]
    } elsif ($a->{y} == $b->{y}) {
        $t->{table}->[($a->{y} + 1) % 5][$a->{x}] .
        $t->{table}->[($b->{y} + 1) % 5][$b->{x}]
    } else {
        $t->{table}->[$a->{y}][$b->{x}] .
        $t->{table}->[$b->{y}][$a->{x}]
    }
}

sub decode_pair {
    my ($t, $pair) = @_;
    my ($a, $b) = (map { $t->{coords}->{$_} } @$pair);
    if ($a->{x} == $b->{x}) {
        $t->{table}->[$a->{y}][($a->{x} - 1) % 5] .
        $t->{table}->[$b->{y}][($b->{x} - 1) % 5]
    } elsif ($a->{y} == $b->{y}) {
        $t->{table}->[($a->{y} - 1) % 5][$a->{x}] .
        $t->{table}->[($b->{y} - 1) % 5][$b->{x}]
```

```
    } else {
        $t->{table}->[$a->{y}][$b->{x}] .
        $t->{table}->[$b->{y}][$a->{x}]
    }
}

sub encode {
    my ($key, $text) = @_;
    my $table = table($key);
    join '', map { encode_pair($table, $_) } split_to_pairs($text)
}

sub decode {
    my ($key, $text) = @_;
    my $table = table($key);
    join '', map { decode_pair($table, $_) } split_to_pairs($text)
}

sub print_as_pairs {
    my $i = 0;
    for (split_to_pairs($_[0])) {
        print join '', @$_;
        print ' ';
        print "\n" unless ++$i % 9;
    }
    print "\n"
}

my $key = 'OIL';
my $res = encode($key, 'BYHAPY');
print_as_pairs($res);
print_as_pairs(decode($key, $res));
```

Результат работы программы:

AZ NO NZ
BY HA PY

Программа так же тестировалась на примере из книги Саломаа А. "КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ"стр. 39, 43.

ключ: OIL

шифротекст:

QN FS LK CM LT HC SM MC VK
IH HA XR QM BQ IE QN AK RD
PS TU CB NX MC IF NX MC IT
YF SD EF IF QN LQ FL YD SB
QN AK EU MC TI IE QN MS IQ
KA PF IL BM WD DF RE IV KA
MC IT QN FX MB FT FT DX AK
HC SM YF WE BA AB QE IV OI
XT IT FM AQ AK QN MX ZU DS

OI XI QN FY RX NV OR RB RA
MC MB NX XM AE OW FT LR NC
IQ QN FM ML SN AH QN QL TW
FL ST LT PI QI QN DS VK AR
FS AQ TI DF SM AK FO XM VA
RZ FT SN GS UD FM SA WA LN
MF IT QN FG LN BQ QE AR VA
DT FT QA AB FY IT MX DK FM
DF QN FX NO XC TF SM FK OY
CM QM BA LH

исходный текст:

TH ET IM EH AS CO ME HE WH
OK NO WS SH OU LD TH IN KI
MU ST GO MY HE AD MY HE AR
TA RE DE AD TH OS EA WF UL
TH IN GS HE RA LD TH EM OR
NI NG OI LP RI CE SD OW NI
HE AR TH EY PL AN AN EW IN
CO ME TA XD AL LA SC OW BO
YS AR EN OT IN TH ES UP ER
BO WL TH AT SW HY IQ UI TI
HE LP MY SE LF IV AN IS HF
OR TH EN EX TM ON TH SO RY
EA RS AS KB RO TH ER WH IT
ET OT RA CE ME IN CA SE YO
UW AN TM EU RG EN TL YI AM
NE AR TH EF AM OU SC IT YO
FR AN TO LA AT AR ES ID EN
CE TH EY HA VE NA ME DN AV
EH SH AL OM

Для криптоанализа необходимо иметь статистику о частоте вхождения пар букв(диграмм) в предложениях языка, на котором написан текст.