现代密码学第一次作业

2050249 徐正扬

2024 年 3 月 24 日

1.1 计算下列数值

- $7503 \mod 81 = 51$
- $(-7503) \mod 81 = 30$
- $81 \mod 7503 = 81$
- $-81 \mod 7503 = 7422$

1.5 使用穷尽密钥搜索方法破译如下利用移位密码加密的密文
BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD
密钥 K=10，明文为 LOOK UP IN THE AIR ITS A BIRD ITS A PLANE ITS SUPERMAN

1.6 在一个密码体制中，如果一个加密函数 e_K 和一个解密函数 d_K 相同，我们将这样的密钥 K 称为对合密钥。试找出定义在 $\mathbb{Z}_{26}$ 上的移位密码的所有对合密钥。
密钥 $K = 13$ 时，$e_K(x) = (x + 13) \mod 26$,$d_K(y) = (y - 13) \mod 26 = (y + 13) \mod 26$
密钥 $K = 0$ 时，显然 $e_K(x) = d_K(y)$

1.7 确定下列定义在 $\mathbb{Z}_m$ 上的仿射密码的密钥量

- $m = 30, \phi(m) = 8$，密钥量 $8 \times 30 = 240$
- $m = 100, \phi(m) = 40$，密钥量 $40 \times 100 = 4000$
- $m = 1225, \phi(m) = 840$，密钥量 $840 \times 1225 = 1029000$

1.9 $1 \leqslant a \leqslant 28$，利用反复试验的方法求出 $a^{-1} \mod 29$ 的值。

a		1	2	3	4	5	6	7	8	9	10	11	12	13	14
a^{-1}	mod 29	1	15	10	22	6	5	25	11	13	3	8	17	9	27
15	16	17	18	19	20	21	22	23	24	25	26	27	28		
2	20	12	21	26	16	18	4	24	23	7	19	14	28		

1.10 已知 $K = (5, 21)$ 是定义在 $\mathbb{Z}_{29}$ 上的仿射密码的密钥

1. 以 $d_K(y) = a'y + b'$ 的形式给出解密函数，这里 $a', b' \in \mathbb{Z}_{29}$。
2. 证明对任意的 $x \in \mathbb{Z}_{29}$，都有 $d_K(e_K(x)) = x$

- $e_K(x) = 5x + 21$,$d_K(y) = 6(y - 21) = 6y + 19$
- $d_K(e_K(x)) = 6(5x + 21) + 19 = 30x + 145 = x$

1.15(a) 求出下列定义在 $\mathbb{Z}_{26}$ 上的矩阵的逆。

$$\begin{pmatrix} 2 & 5 \\ 5 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 5 \\ 5 & 9 \end{pmatrix}^{-1} = \begin{pmatrix} 11 & 15 \\ 1 & 20 \end{pmatrix}$$

1.16 设下列的 π 是集合 $1, 2, \cdots, 8$ 上的置换:

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

1. 求出逆置换 π^{-1}
2. 解密下列使用置换密码加密的密文，密钥是 (a) 中的置换 π

$$TGEEMNELNNTDROEOAAHDOETCSHAEIRLM$$

x	1	2	3	4	5	6	7	8
π^{-1}	2	4	6	1	8	3	5	7

- $GENTLEMENDONOTREADEACHOTHERSMAIL$
  (Gentlemen do not read each others mail)

1.18 考虑下列定义在 $\mathbb{Z}_2$ 上的四级线性递归序列

$$z_{i+4} = (z_i + z_{i+1} + z_{i+2} + z_{i+3}) \mod 2, i \geqslant 0$$

对其 16 种可能的初始向量 $(z_0, z_1, z_2, z_3) \in (\mathbb{Z}_2)^4$，分别求出其生成的密钥流的周期。

(z_0, z_1, z_2, z_3)	周期
0000	1
0001	5
0010	3
0011	20
0100	20
0101	5
0110	3
0111	9
1000	17
1001	11
1010	5
1011	3
1100	33
1101	14
1110	80
1111	80

1.19 令递归关系式为

$$z_{i+4} = (z_i + z_{i+3}) \mod 2, i \geqslant 0$$

重新完成 1.18 中的问题。

除 $(0, 0, 0, 0)$ 的周期为 1 外，其余 15 种初始向量的密钥流周期均为 15。

补充题 b1.1 你认为安全的密码算法的该如何定义？请写出自己的思考。

安全的密码算法我认为应该要求密钥空间足够大，算法需要一定的复杂性，并且能够抵御各种密码分析以及明文攻击方式。

思考题 s1.1 把应用于维吉尼亚密码的重合指数法应用到仿射密码的唯密文密码分析中，请写出分析算法步骤，及实现代码。测试明文 (测试时请去掉空格)，或使用课本第 1 章习题 1.21 中的仿射密码密文 (c) 来测试:

This is an essay I wrote for a mathematics essay prize We had a number of possible topics to choose from and I choose cryptology because I already had a passing interest in thanks to my attempts to code encryption algorithms for my computer programs It won by the way This is the original essay with a few corrected spelling mistakes though there are probably some left am currently studying at Imperial College my home page is here

1.21(c): KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUPKRIOFKPACUZQEPBKRXPEIIEABDKPBCPFCDCCAFIEABDKPBCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFFERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERKIVKSCPICBRKIJPKABI

验证明文较为简单，编写代码如下

```
int main() {
    string s("THISISAN...HERE");

    auto f = [&](const string &p) {
        int n = (int) p.size();
        vector<int> cnt(26);

        for (auto &i: p)
            ++cnt[i - 'A'];

        double ret = 0;
        for (auto &i: cnt)
            ret += i * (i - 1);

        return ret / (n * (n - 1));
    };

    cout << f(s) << endl;
}
```

此时得到 $I_c(x)$ 的值为 0.0626243，非常接近 0.065。

用重合指数法分析仿射密码的代码实现如下，

```
    const vector<double> a({0.082, 0.015, 0.028, 0.043, 0.127, 0.022, 0.020, 0.061, 0.070, 0.002, 0.008, 0.040, 0.024,
                    0.067, 0.075, 0.019, 0.001, 0.060, 0.063, 0.091, 0.028, 0.010, 0.023, 0.001, 0.020, 0.001});
    auto f = [&](const string &p) {
        int n = (int) p.size();
        vector<int> cnt(26);

        for (auto &i: p)
            ++cnt[i - 'A'];

        double ret = 0;

        for (int i = 0; i < 26; ++i) {
            ret += a[i] * cnt[i];
        }
        return ret / n;
    };
```

```
for (int i = 0; i < 26; ++i) {
    if (gcd(i, 26) != 1)
        continue;
    for (int j = 0; j < 26; ++j) {
        for (int k = 0; k < n; ++k) {
            t[k] = char((qpow(i, 11) * (s[k] - 'A' - j + 26)) % 26 + 'A');
        }
        cout << i << '␣' << j << '␣' << f(t) << endl << t << endl;
    }
}
```

函数返回的结果就是 M_g 的值，观察结果得到一个接近 0.065 的值，当 $a = 19, b = 4$ 时，$M_g = 0.0699444$。

此时得到的明文为 OCANADATERREDENOSAIEUXTONFRONTESTCEINTDEFLEURONSGLORIEUXCARTONBRASSAITPORTERLEPEEILSAITPORTERLACROIXTONHISTOIREESTUNEEPOPEEDESPLUSBRILLANTSEXPLOITSETTAVALEURDEFOITREMPEEPROTEGERANOSFOYERSETNOSDROITS

翻译为 Ô CANADA! Terre de nos aïeux, Ton front est ceint de fleurons glorieux! Car ton bras sait porter l'épée, Il sait porter la croix! Ton histoire est une épopée des plus brillants exploits. Et ta valeur, de foi trempée, protégera nos foyers et nos droits! 这是法语版本的加拿大国歌。