2024-2025学年《密码学》期末考试

1　判断题(2分一个)

1.Z_3上的可逆矩阵数量为48

2.扩展欧几里得的时间复杂度为$O(k^3)$

3.RSA是语义安全的。

4.对于维吉尼亚加密，直接可以使用频率分析来求解明文。

5.有关熵，一个密钥在全部是平均的时候，熵是最小的

6.忘了

7.忘了

8.sm2和sm3分别用了什么密钥体制来进行加密。

9.公钥加密比对称加密要来的安全。

10.AES的三种密钥方案，对应的明文分组长度是一样的。

2　填空题

（5分）1.Z_{35}中的伪平方数有几个?

（5分）2.简单的$rabin$密码体系的已知密文求明文

3　解答题

（10分）1.课本1.19原题，流加密的周期求解

1.19　令递归关系式为：

$$z_{i+4} = (z_i + z_{i+3}) \bmod 2$$

$i \geqslant 0$。重新完成习题 1.18 中的问题。

（10分）2.课本上的原题，很偏。。。关键是要写出为什么极限是0，不太好弄，这一块刚好没复习，直接凉凉

例 8.3 假设一个比特生成器 f 仅产生刚好 $\ell/2$ 个比特为 0，$\ell/2$ 个比特为 1 的 ℓ 长比特序列。定义函数 dst 为

$$\mathrm{dst}(z_1,\cdots,z_\ell)=\begin{cases}1 & \text{如果 } (z_1,\cdots,z_\ell)\text{ 恰有 } \ell/2 \text{ 个比特为 } 0\\ 0 & \text{其他}\end{cases}$$

不难看出，此时有

$$E_{\mathrm{dst}}(p_u)=\frac{\binom{\ell}{\ell/2}}{2^\ell}$$

且

$$E_{\mathrm{dst}}(p_f)=1$$

可以证明

$$\lim_{\ell\to\infty}\frac{\binom{\ell}{\ell/2}}{2^\ell}=0$$

因此，对任意固定的 $\epsilon<1$，如果 ℓ 是充分大的，那么 p_u 和 p_f 是 ϵ 可区分的。

（10分）3.hash碰撞，作业原题应该是

4.10 在这个习题中，我们考虑 Derkle-Damgård 结构的一个简化版本。假定

$$\text{compress}: \{0,1\}^{m+t} \to \{0,1\}^m$$

其中 $t \geqslant 1$，假定

$$x = x_1 \| x_2 \| \cdots \| x_k$$

其中

$$|x_1| = |x_2| = \cdots = |x_k| = t$$

我们研究下面的迭代 Hash 函数：

算法 4.9 简化的 Merkle-Damgård(x, k, t)

external compress

$z_1 \leftarrow 0^m \| x_1$

$g_1 \leftarrow \textbf{compress}(z_1)$

for $i \leftarrow 1$ **to** $k-1$

do $\begin{cases} z_{i+1} \leftarrow g_i \| x_{i+1} \\ g_{i+1} \leftarrow \textbf{compress}(z_{i+1}) \end{cases}$

$h(x) \leftarrow g_k$

return $(h(x))$

假定 compress 是碰撞稳固的，进一步假定 compress 是零原像稳固的，也就是说，难以找到满足 $\text{compress}(z) = 0^m$ 的 $z \in \{0,1\}^{m+t}$。在这些假定条件下，证明：h 是碰撞稳固的。

（15分）4.计算一个ECDSA，基本和信安数基的是一样的，不过也很难算

- 计算$y^2 = x^3 + x + 6 (mod\ 11)$的阶数，应该算出来是13，第二问要用
- 根据提供的数据，计算数字签名，算错一步就寄，前提还得是第一问得算对，如果第一问错了，也是15分全扣好吧

（15分）5.默写椭圆曲线的密钥体制。。。然后证明其安全性

这题首先你得会背ElGamal的体制，如果没背的话直接15分全扣，凉凉

密码体制 6.1　$\mathbb{Z}_p^*$ 上的 ElGamal 公钥密码体制

设 p 是一个素数，使得 $(\mathbb{Z}_p^*, \cdot)$ 上的离散对数问题是难处理的，令 $\alpha \in \mathbb{Z}_p^*$ 是一个本原元。令 $\mathcal{P} = \mathbb{Z}_p^*$，$\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$，定义

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a \pmod p\}$$

p, α, β 是公钥，a 是私钥。

对 $K = (p, \alpha, a, \beta)$，以及一个(秘密)随机数 $k \in \mathbb{Z}_{p-1}$，定义

$$e_K(x, k) = (y_1, y_2)$$

其中

$$y_1 = \alpha^k \bmod p$$

且

$$y_2 = x\beta^k \bmod p$$

对 $y_1, y_2 \in \mathbb{Z}_p^*$，定义

$$d_K(y_1, y_2) = y_2(y_1^a)^{-1} \bmod p$$

然后证明安全性，书上有，但是很抽象

我觉得他的意思应该是，如何把椭圆曲线的难解性图灵规约到DLP难解性问题上（不知道）

（10分）6.SM4计算，涉及到有限域求逆，很难算

- 第一问8分，算75的SM4加密结果，关键就是怎么算SM4下的有限域的75的逆元
- 第二问2分，算00的SM4加密结果，00的逆就是00，这样好求一些

类似于这样：