2022学期《密码学原理》期末考试试卷

*本次考试为开卷考试，可以查阅各种资料（包括网络），但请独立完成作答。

**请大家在北京时间2022年12月28日早上8点前，将解答发送至191220003@smail.nju.edu.cn，并抄送一份至zhangyuan@nju.edu.cn. 请将邮件名和附件文件命均名为"学号_姓名_密码学"

***答题可以在纸上手写然后拍照，请保持字迹清晰并注明题号；也欢迎大家使用markdown，latex等编辑软件书写答案（提供试卷的markdown文件）

姓名：_____ 学院: _____ 学号: _____

1.(10 points)

请判断以下函数是否为可忽略的(negligible)，并证明你的结论。

(a) $f(n)=\frac{1}{2^{2022\log n}}$

(b) $f(n)=\frac{1}{\sqrt[2022]{n!}}$

2.(15 points)

请判断以下构造的函数**是否一定**是伪随机数生成器（pseudorandom generator）？并简要说明理由。

（a） 如果f_1和f_2是两个不同的伪随机数生成器，定义$g(x)=f_1(x)||f_2(\overline{x})$，其中$\overline{x}$表示对比特串$x$按位取非，$||$表示比特串拼接。

（b） 如果f是伪随机数生成器，定义$g(x)=f(x)||f(\overline{x})$。

（c） 如果f是输出长度为$l(n)>n$的伪随机数生成器，定义$g(x)=f(x)\oplus(x||0^{l(|x|)-|x|})$，其中$\oplus$表示按位异或运算，$|x|$表示比特串$x$的长度。

3.(15 points)

计算题（不允许使用计算机、计算器、手机等电子设备）

（a）在Plain RSA密码系统中，假设模(modulus) $N=77$，加密指数$e=13$，明文$m=3$，那么m对应的密文$c=$_____。

（b）在Plain RSA密码系统中，假设模$N=77$，加密指数$e=43$，密文$c=3$，则解密密钥$d=$____，密文c对应的明文$m=$____。

（c）在ElGamal密码系统中，假设G是以$p=17$为模的乘法群。如果明文m的密文为$(4,11)$，明文m'的密文是$(6,5)$，那么请分别构造$2m$的一个密文_____，mm'的一个密文_____。

4.(20 points)

参考讲义中ElGamal加密系统的密钥生成算法Gen, 可以构造如下一个新的"1比特加密方法": 若公钥为 $(\mathbb{G},q,g,h)$, 私钥为$(\mathbb{G},q,g,x)$，其中q为$\mathbb{G}$的阶，g为其生成元，x等概率选取于$\mathbb{Z}_q$。

对于明文 $b \in \{0,1\}$

- 若$b=0$, 则等概率独立选取随机数 $y,z \in \mathbb{Z}_q$, 并计算 $c_1 := g^y, c_2 := g^z$，密文为 $\langle c_1, c_2 \rangle$.
- 若$b=1$, 则等概率选取一个随机数 $y \in \mathbb{Z}_q$, 并计算 $c_1 := g^y, c_2 := h^y$，密文为 $\langle c_1, c_2 \rangle$.

请回答以下问题:

(1) 证明若 DDH 问题关于$\mathbb{G}$ 是困难的, 那么该加密系统是 CPA 安全的.

(2) 考虑这样一个群$\mathbb{G}'$:

- 考虑模p的乘法群$\mathbb{Z}_p^*$，其中$p=2q+1$且p,q都是素数. 令集合$\mathbb{G}' = \{x \in \mathbb{Z}_p^* : \exists y \in \mathbb{Z}_p^*, y^2 = x\}$

容易验证$\mathbb{G}'$也是$\mathbb{Z}_p^*$上的乘法群。

请问我们构造的加密算法在$\mathbb{G}'$上也是CPA安全的吗？请证明你的结论。

5.(20 points)

定义一个签名方案$(Gen, Sign, Verfy)$ 如下：

- Gen: 依照ElGamal密钥生成算法生成(g,y,x,q)。q是一个大质数；g是$\mathbb{Z}_q^*$的一个随机的生成元（generator）;$x \xleftarrow{R} \mathbb{Z}_{q-1}, y = [g^x \mod q]$; 公钥$pk = (g,y,q)$，私钥$sk = (g,x,q)$, 其中$\xleftarrow{R}$表示按均匀分布随机从集合选取。
- $Sign(m)$: $k \xleftarrow{R} \mathbb{Z}_{q-1}; r = [g^k \mod q]$; $s = [(km - x) \mod (q-1)]$
  如果$s=0$，则重新签名；否则，输出$\sigma = (r,s)$.
- $Verfy(m,\sigma)$: 如果$0<r<q, 0<s<q-1$, 且$r^m = yg^s \mod q$ 输出1；否则输出0。

(1）请判断以上签名方案是否安全？如果安全，请严格证明；否则，给出一个攻击方案。

(2）判断下一方案是否安全？如果安全，请给出严格证明；否则，请给出一个攻击方案。

- $Sign(m)$: $k \xleftarrow{R} \mathbb{Z}_{q-1}^*; r = [g^k \mod q]$; $s = [(m - xr)k^{-1} \mod (q-1)]$
  如果$s=0$，则重新签名；否则，输出$\sigma = (r,s)$.
- $Verfy(m,\sigma)$: 如果$0<r<q, 0<s<q-1$, 且$g^m = y^r r^s \mod q$ 输出1；否则输出0。

6.(20 points)

在今年的全球开发者大会上，苹果宣布于9月份开始在Mac、iPhone、iPad和Apple TV上推出无密码（None-Password）登录。在iOS 16和MacOS Ventura上，人们不再使用密码(Password)，而是使用Passkey登录网站和应用。这是现实世界中为消除密码而进行的第一次重大转变。请去互联网上简单调研Passkey技术，并简要论述一下：

(1）基于Password和基于Passkey方案的在安全性上的主要区别；（请尽量将答案控制在60字以内）

(2）结合密码学课上学到的知识，你能否大体描述一下Passkey方案是如何避免向身份验证服务器泄漏密钥信息，又能完成身份验证的？（请尽量将答案控制在60字以内）