Crypto_Midterm_2023Fall

`Problem.1` 在使用凯撒密码加密小写字母时，我们的密钥空间为 $[0,25]$ 中的整数。
`(1)` 证明如果密钥空间为 $[0,29]$ 中的整数，则该方案是不完美保密的。
`(2)` 更改 `KEYGEN` 算法使得使用 $[0,29]$ 中的整数作为密钥空间是，方案是完美保密的。

`Problem.2` 判断下列函数是否为可忽略函数，对于后两问给出简要说明。
`(1)` $f_1=2^{-\sqrt{logn}}$
`(2)` $f_2=n^{-log\ log\ logn}$
`(3)` $f_3=\frac{n!}{n^n}$
`(4)` $f_4=(g(n))^n$，其中 $g(n)$ 是一个值域在 $(0,1)$ 上的严格单调减的不可忽略函数
`(5)` $f_5=g(h(n))$，其中 $g(n)$ 和 $h(n)$ 都是可忽略函数

`Problem.3` 设一伪随机数生成器 $G:\{0,1\}^n\to\{0,1\}^{2n}$，令 $G'=G(x)_{[0,n)}||G(G(x)_{[n,2n)})$。证明 G' 是一个伪随机数生成器或给出反例。

`Problem.4` 设 Π 是一个 CPA 安全的加密方法，定义 $Enc_k\Pi'(m)=Enc_k\Pi(m)||\texttt{LSB}(k)$。其中 `LSB(k)` 是 k 的二进制最低位。证明 Π' 是 CPA 安全的或给出反例。

`Problem.5` 我们仿照 CBC-MAC 的流程，基于 OFB 模式定义 OFB-MAC 认证方法：

- 使用随机的 IV 和 k 作为算法初值，使用 $M=m_1||m_2||\dots||m_n$ 作为输入
- 令 $IV_i=F_k(IV_{i-1})$，特别地，令 $IV_0=IV$
- 令 $c_i=m_i\oplus IV_i$
- 令 $t=c_1\oplus c_2\oplus\dots\oplus c_n$，作为 $MAC_k(M)$ 的 `tag` 输出
  `(1)` 假设你拥有 $MAC_k(\cdot)$ 的神谕机，设计一种方法得到 $F_k(IV)$。
  `(2)` 假设你拥有了 IV、$F_k(IV)$，设计一组输入使得输出的 `tag` 是给定的 h。