

密码学组队学习第四期

2023.09.02

1 (NSUCRYPTO 2021 Section A Problem 1)

请破译下面的密码

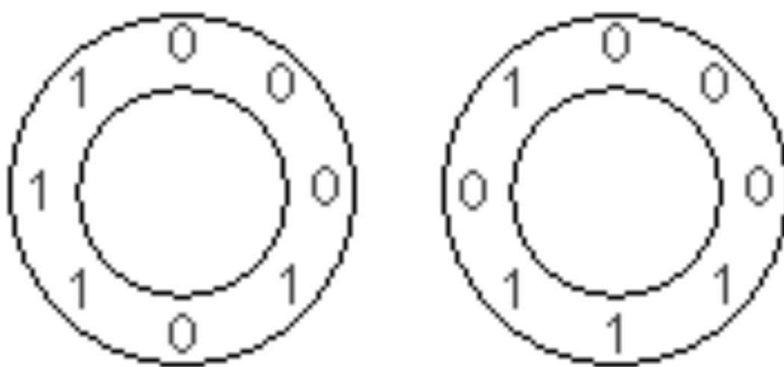
● ● ● ● ● ● ●
V R L E A T D _ I E M Q U
I I R P _ M K E O N T T _
E S L O N B I O K L O - P
V . , _ _ I S T O _ V W A
I S E _ T N _ O S T C _ D
I E E C N R T Y I P S T E
T D , _ _ D I U N R V I N
E G N _ T T E H D E _ _ S
T E H C E O _ N U D N _ W
I O Q R U L E D _ _ S W A
E R C .

2 新的需求

某天，小明收到产品经理发来的需求，需要设计一个压缩算法，将加密后的密文进行压缩，以减少通信量，提升效率。你给小明推荐一个呗。

3 (Project Euler Problem 265) 二进制圆圈

长度为 2^N 的比特串可以排成一圈，使得任意 N 个相邻比特构成的子串（按顺时针方向）都不一样。例如，对 $N = 3$ ，不考虑旋转的情况下，有两种不同的圆排列，如下图所示。



得到的长度为 3 的比特串分别为: 000, 001, 010, 101, 011, 111, 110, 100. 这样, 每个圆排列都可以编码为从 N 个 0 开始, 顺时针方向对应的比特串对应的数字。如上图中, 两个圆排列对应的数字分别是 $(00010111)_2 = 23$, $(00011101)_2 = 29$ 。令 $S(N)$ 为所有满足条件的圆排列对应的数字的和。计算 $S(5)$ 。

4 SM2 分布式签名算法

SM2 是我国的商用密码标准算法，可以提供数字签名、公钥加密、密钥封装等功能。小白最近设计了一个两方的 SM2 分布式签名协议。请找出其中安全漏洞（下面的协议描述不完整，请先不要尝试解决）。

- 分布式密钥生成
 1. Alice 随机选取 $D_1 \in [1, n-1]$
 2. Bob 随机选取 $D_2 \in [1, n-1]$, 计算 $P_1 = (D_2 + 1)^{-1}G$, 将 P_1 发送给 Alice。
 3. Alice 计算公钥 $P = (D_1 + 1)^{-1}P_1 - G$ 。
- 分布式签名
 1. Alice 将待签名的消息 M 进行预处理得到 e 。生成随机数 $k_1 \in [1, n-1]$, 计算 $Q_1 = k_1G, w_1 = k_1(D_1 + 1)^{-1}G$, 将 Q_1, w_1, Q_2 发送给 Bob。
 2. Bob 计算得到 $r = (x_1 + e), s_1 = (k_2 + 1)(D_2 + 1), s_2 = r(D_2 + 1) + k_2$, 发送给 Alice。
 3. Alice 计算 $s = k_1s_1 + (D_1 + 1)k_1 + (D_1 + 1)s_2 - r$ 。输出 M 的签名 (r, s) 。

5 基于比特切片的高吞吐 SM4 算法实现

6 一台坏掉的 RSA 解密机

7 基于 SIMD 指令集的高效模运算实现

8 Oblivious Transfer Extension Explained