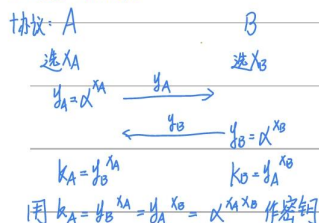


如果把 K_A 或 K_B 当作密钥会出现什么问题？实例说明：对 P 和 $GF(P)$ 具体群，是否满足 ppt 前面对密钥的要求

Diffie-Hellman

对密钥的要求：随机，长周期，独立性，非线性



构造 $GF(11) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $\alpha = 2$, $p = 11$

① 随机 \rightarrow

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | $\rightarrow X_A$ |
|-----------------------------------|----|---|----|----|----|----|----|----|----|----|----|-------------------|
| $\alpha^0 = 1$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| $\alpha^1 = 2$ | 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $\alpha^2 = 4$ | 2 | 0 | 2 | 4 | 6 | 8 | 10 | 1 | 3 | 5 | 7 | 9 |
| $\alpha^3 = 8$ | 3 | 0 | 3 | 6 | 9 | 1 | 4 | 7 | 10 | 2 | 5 | 8 |
| $16 \leftarrow \alpha^4 = 5$ | 4 | 0 | 4 | 8 | 1 | 5 | 9 | 2 | 6 | 10 | 3 | 7 |
| $32 \leftarrow \alpha^5 = 10$ | 5 | 0 | 5 | 10 | 4 | 9 | 3 | 8 | 2 | 7 | 1 | 6 |
| $64 \leftarrow \alpha^6 = 9$ | 6 | 0 | 6 | 1 | 7 | 2 | 8 | 3 | 9 | 4 | 10 | 5 |
| $128 \leftarrow \alpha^7 = 7$ | 7 | 0 | 7 | 3 | 10 | 6 | 2 | 9 | 5 | 1 | 8 | 4 |
| $256 \leftarrow \alpha^8 = 3$ | 8 | 0 | 8 | 5 | 2 | 10 | 7 | 4 | 1 | 9 | 6 | 3 |
| $512 \leftarrow \alpha^9 = 6$ | 9 | 0 | 9 | 7 | 5 | 3 | 1 | 10 | 8 | 6 | 4 | 2 |
| $1024 \leftarrow \alpha^{10} = 1$ | 10 | 0 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

X_B

统计 $(X_A \cdot X_B) \bmod p$ 结果中各个数字出现的次数发现 0 出现 21 次，其余数字 10 次

由此可见 $\alpha^{X_A X_B} \bmod p$ 所得密钥 K 的取值分布并不等概率随机。

因此所得密钥不具备随机性 且若一方选择 $X=0$ 则最终 $K = \alpha^0 = 1$

攻击者可以通过得到 $Y_A \neq 1$ 来大致推断最终密钥是否也为 $\alpha^0 = 1$