# Q1 Crypto

This CTF challenge is related to the Discrete Logarithm Problem (DLP), focusing on how its security is established. The challenge tests your understanding of asymmetric encryption by using an outdated encryption bit-width. [(How to generate this?)](https://github.com/FrogGuaGua/SQRPRGRM/blob/main/CTFanswer%26design/Q1/design.js)  


Figure 1 DLP

## POC:

1. **Factorizing large numbers**

Tools: [yafu](https://github.com/bbuhrow/yafu) (or any tool)

Key in

factor(0xb6d733a404d0b06e51dcf52fec53b6b9ed807b3bdc13dbe33e5e59182f66b733)

We get

A screenshot of a computer screen

Description automatically generated

Figure 2 p and q

Prime1 = 244797265212401102686995522653336482037

Prime2 = 337835338562002625014208649165305613959

1. **Calc φ**p **= (**Prime1**-1)\*(** Prime2**-1)**  
   φp = 82701166972083873963502681321091904267252851881480149626751213724120817858488
2. Start calc G (true message)  
   Tools: [RDLP (windows only)](https://github.com/FrogGuaGua/SQRPRGRM/tree/main/CTFanswer%26design/Q1/RDLP_v1.07)

A screenshot of a computer

Description automatically generated

Figure 3 get G

We get answer 486163656B343072457173.

1. Verification



Figure 4 final flag

[Attack Script](https://github.com/FrogGuaGua/SQRPRGRM/blob/main/CTFanswer%26design/Q1/answer.js)