

BUUCTF-Crypto-RSA大全

原创



VIP文章 [ASSOINT](#)



于 2020-12-14 20:35:17 发布



711



收藏 2

分类专栏: [Crypto](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_47869330/article/details/111184585

版权

RSA算法

密文=明文的E次方除以N取余数

E=Encryption(加密)

N=Number(数字)

所以: 公钥=(E,N)

明文=密文的D次方除以N的余数

D=Decryption(解密)

所以: 私钥=(D,N)

N=p