Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Rsa\_oracle – picoCTF

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Rsa\_oracle – Guilherme Gonsales de Sá |
| **N° Revisão** | 1 |
| **Data de publicação** | 25/05/2025 |
| **Link** | <https://play.picoctf.org/practice/challenge/422?category=2&difficulty=2&page=1> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Guilherme Gonsales de Sá | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 24/05/2025 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

|  |  |
| --- | --- |
| **Informações do CTF** | |
| **Nível de Dificuldade** | Médio |
| **Tipo de acesso** | Gratuito |
| **Conceitos envolvidos** | Criptografia |
| **Plataforma** | picoCTF |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Desenvolvimento 3](#_heading=h.1fob9te)

[Conclusão 5](#_heading=h.1t3h5sf)

[Referências 5](#_heading=h.4d34og8)

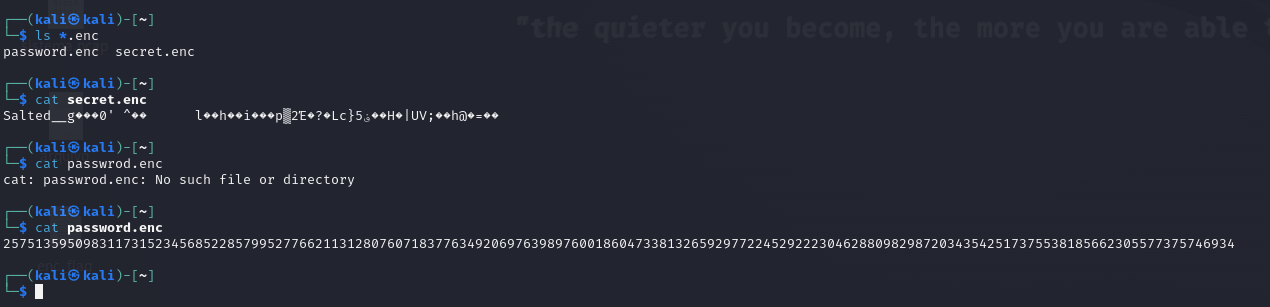
Scripts 5

**Contextualização**

O rsa\_oracle é um ctf onde devemos manipular a chave RSA de forma que obtenhamos a mensagem original. O ctf é um bom exemplo de uma aplicação real da criptografia em um cenário verossímil, por isso é se mostra interessante.

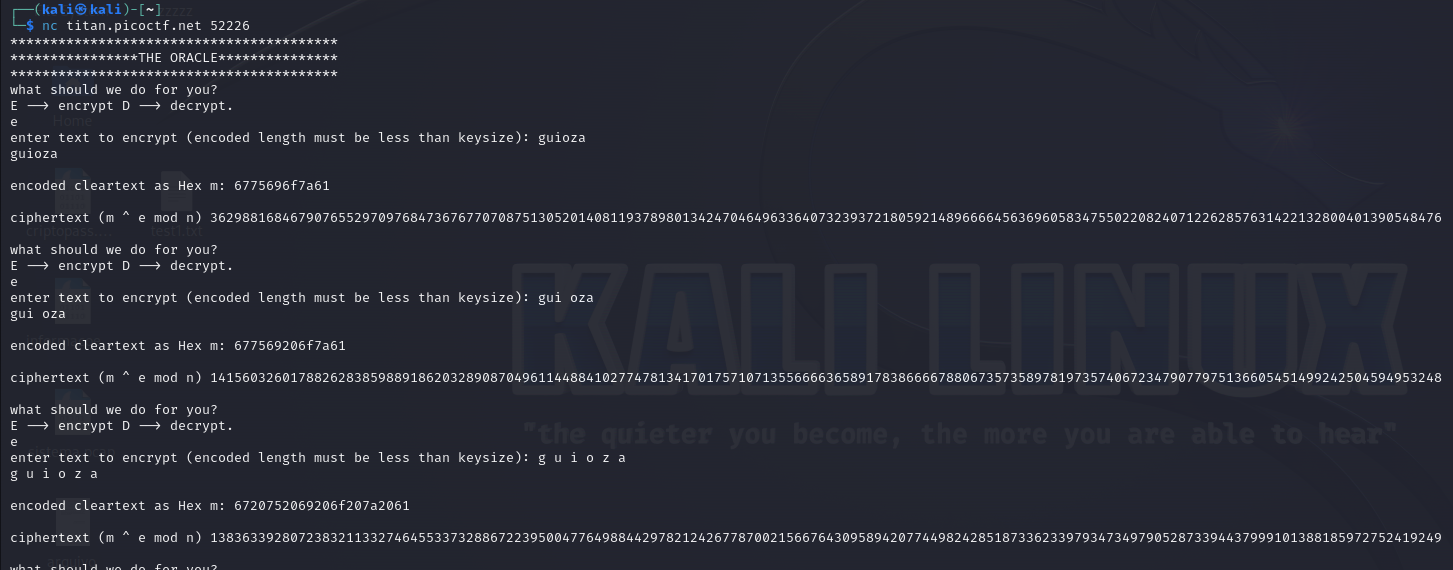
**Desenvolvimento**

De início, baixemos os arquivos indicados necessários e vejamos seus conteúdos.

****

Observa-se que no arquivo *secret.enc* obtem-se algo que, ao que tudo indica, é uma criptografia com um salt. Em primeiro momento, pode-se imaginar que é um salted hash, mas não nos preocupemos com isso agora.

Em *password.enc* observa-se uma chave encriptada, aparentemente no formato RSA.



Acima estão alguns exemplos da encriptação do oráculo. No entanto, não consegue-se derivar muito disso.

Sabe-se que o oracle não consegue decriptar a chave diretamente. Sendo assim, deve-se tentar fazer com que ele a decripte sem o comando direto.

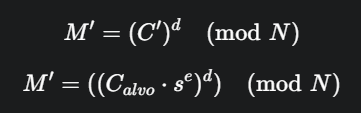
Tentemos um *ataque de blinding*. Ataques de blinding podem ser feitos em oráculos e consistem em tentar obter uma informação sem que a mesma seja estritamente requisitada.

A ideia do ataque é: cifrar uma string conhecida, utilizar a string cifrada como fator adicional de encriptação da string desejada, decriptar a mensagem com o próprio oráculo e, por fim, reverter a modificação da string desejada. Dado que computadores compreender caracteres de forma algébrica, isso se torna possível devido a reversibilidade dessas operações.

De forma genérica, pode-se entender um ataque de blinding da seguinte forrma:







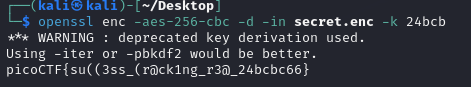




Sendo assim, façamos um script que faça o processo de blinding. Ao rodar o script, somos retornados a chave utilizada.



Utilizemos agora o arquivo *secret.enc,* com a chave que encontramos.. Estamos utilizando *openssl* pois sabemos pela dica fornecida que o software possui ferramentas para resolver. Pode-se utilizar o seguinte comando, utilizando a flag *-k* para indicar a chave encontrada, tem-se:



Dessa forma, resolvemos o exercício e encontramos a flag.

ADENDO: Para cada inicialização do servidor, a flag mudará.

**Conclusão**

Apesar de não ser complexo em conceito, o ctf demonstra como é possível aplicar encriptação RSA na prática, além de uma necessidade do domínio de álgebra (reversibilidade de operações, por exemplo) além da aplicação de táticas para enganar softwares pré-existentes.

**Scripts**

1 – script de blindng (pode-se alterar as URLs e portas, além das verificações).

****

**Referências**

<https://github.com/noamgariani11/picoCTF-2024-Writeup/blob/main/Cryptography/rsa_oracle.md> -- Script