Entropia de Geradores Pseudo-Aleatórios no Sistema Criptográfico RSA

Apresentadores: Felipe Gurgel Araujo, Pedro Francisco Staino Santayana

Objetivo do Trabalho

Explorar a geração de chaves RSA e calcular a entropia.

1

Objetivo

Utilizar a Regra de Simpson 3/8.

Introdução à Criptografia RSA

Método popular de criptografia.

RSA

Emprega chaves públicas e privadas.

Segurança

Avaliada através da entropia

Metodologia - Geração de Chaves RSA

Biblioteca Utilizada: cryptography

Tamanho das Chaves

2048 bits.

Código

Exemplo de geração de chaves RSA.

```
def generate_rsa_key():
        private_key = rsa.generate_private_key(
                public_exponent=65537,
                key_size=2048,
        )
        public_key = private_key.public_key()
        return public_key
# Gerar um conjunto de chaves
num_keys = 1000 keys = [
        generate_rsa_key()
        for _ in range(num_keys)
]
```

Serialização e Contagem de Frequências

1

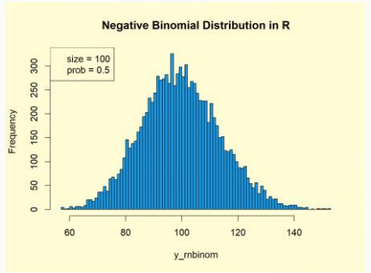
Serialização

Transformar chaves em formato comparável.

2

Contagem

Análise da frequência das chaves.



Cálculo da Entropia

Fórmula de Shannon

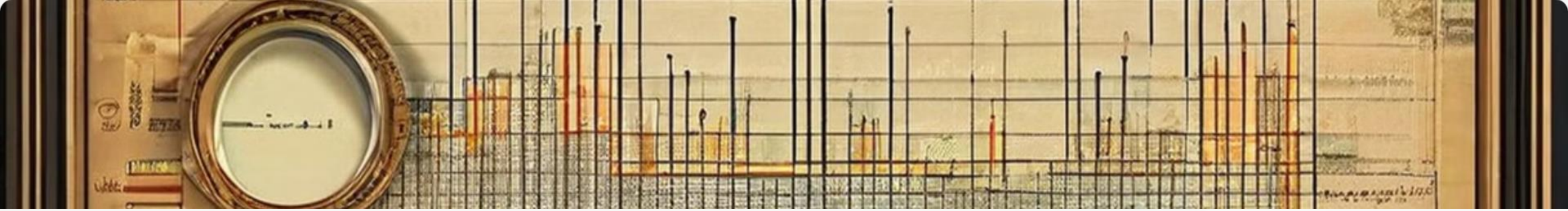
$$\mathrm{H(x)} = -\Sigma p(x) \cdot log2\, p(x) dx$$

p(x) = frequência da chave / número total de chaves

Regra de Simpson

Integrando as chaves após usar a formula de Shannon

$$-\int p(x) \cdot log2\, p(x) dx$$



Código para Regra de Simpson 3/8

Código

```
def simpsons_3_8_rule( f, a, b, n ):
    if n % 3 != 0:
        n += 3 - (n % 3)    # (n) deve ser múltiplo de 3
    h = (b - a) / n
    integral = f(a) + f(b)
    for i in range( 1, n ):
        xi = a + i  * h
        if i % 3 == 0:
            integral += 2  f(xi)
        else:
            integral += 3  f(xi)
    return ( 3 *  h  /  8 ) * integral
```

Valor Recomendado de Entropia

1 **Recomendação**

log2(n) para n chaves únicas.

2 **Exemplo**

Para 1000 chaves, o valor recomendado é log2(1000).

Resultados

print(f"A entropia calculada das chaves RSA é: {entropy_value} bits")

Entropia Calculada	Valor Recomendado
A entropia calculada das chaves RSA é: 9.955818500378426 bits	O valor recomendado de entropia para 1000 chaves é: 9.97 bits

Conclusão

1 **Eficiência e Segurança**

Validação do método.

2 **Importância da Entropia**

Garantia da robustez das chaves.