Implementação e Ataque da Cifra de Vigenère

Thales Lima Menezes e Rafael dos Santos Silva
Dep. Ciência da Computação
Universidade de Brasilia
Brasília, Brasil
170045919@aluno.unb.br, 180129716@aluno.unb.br

***Resumo*—Este trabalho detalha uma implementação dos algoritmos criptográficos AES-CTR e RSA. É também explicada a implementação dos algoritmos propostos, escrita em Python.**

***Index Terms*—cifra, AES, AES-CTR, RSA, criptografia**

I. Introdução

RSA (Rivest-Shamir-Adleman) é um dos primeiros sistemas de criptografia de chave pública e é amplamente utilizado para transmissão segura de dados. Neste sistema de criptografia, a chave de encriptação é pública e é diferente da chave de decriptação que é secreta (privada). No RSA, esta assimetria é baseada na dificuldade prática da fatorização do produto de dois números primos grandes, o ”problema de fatoração”.

O padrão de criptografia avançada - advanced encryption standard (AES), é uma especificação para a criptografia de dados eletrônicos estabelecida pelo instituto nacional de padrões e tecnologia dos E.U.A. (NIST) em 2001.

O AES foi adotado pelo governo dos Estados Unidos da América. Ele substitui o padrão de criptografia de dados (DES), que foi publicado em 1977. O algoritmo descrito pelo AES é um algoritmo de chave simétrica, o que significa que a mesma chave é usada para criptografar e descriptografar os dados. No modo de operação CTR (Counter), é usado como um bloco de entrada para o criptografador (Encrypt), o valor de um contador (Counter, Counter + 1,. . . , Counter + N – 1).

O contador tem o mesmo tamanho do bloco usado e a operação XOR com o bloco de texto simples é realizada no bloco de saída do criptografador. Todos os blocos de criptografia usam a mesma chave de criptografia. Como este modo, não será afetado pelo bloco quebrado e se você puder obter o contador diretamente, poderá criptografar/descriptografar dados em paralelo.

Neste trabalho, foi desenvolvido um programa que possibilita a cifração e decifração de uma mensagem com RSA e AES no modo CTR, que é descrito na seção **??**. Além disso, é descrito um método de ataque à cifra, que tenta automaticamente descobrir a chave com a qual um texto foi cifrado, na seção **??**.

II. Estruturação do Projeto

Neste trabalho, foi implementado um codificador e decodificador com várias bibliotecas de auxilio, sendo o arquivo principal o *testar.py*. O projeto foi construído utilizando a versão 3.10.4 e testado em Linux.

III. Conclusão

Neste trabalho, foram introduzidos os algoritmos AES-CTR e RSA, podendo explorar conceitos de criptografia modernos utilizados em protocolos como HTTPS e WhatsApp para criptografias de chave pública e privada.