Trabalho 1
Programação Assembler

Luana Cruz Silva, 20/2033543

[1]Dep. Ciência da Computação – Universidade de Brasília (UnB)
CiC - Organização e Arquitetura de Computadores

Resumo. *O objetivo do trabalho é implementar em assembler do RISCV, utilizando o ambiente RARS para programação e teste do software, um algoritmo partir de um código C que descreve parte do algoritmo de cifragem de dados IDEA.*

1. Repositório

`https://github.com/luacrz/OAC-T1-AlgoritmoIDEA.git`

2. O que foi feito

O código implementa uma operação IDEA (International Data Encryption Algorithm) em um conjunto de blocos de entrada (blk-in) usando chaves (keys) e armazenando os resultados em um bloco de saída (blk-out).

2.1. Seção .data

Definição das variáveis de dados: blk-in: Um bloco de entrada com quatro palavras de 32 bits. blk-out: Um bloco de saída onde os resultados serão armazenados. keys: Uma sequência de chaves usadas no processo. output-format: Uma string de formato usada para impressão dos resultados.

2.2. Seção .text

Código executável principal do programa.

2.2.1. main

: Inicializa os registradores (t0, t1, t2) com os endereços das variáveis de dados.

2.2.2. Chamada da Função idea-round

O programa faz uma chamada para a função idea round usando jal. Esta função executa uma única rodada da operação IDEA nos blocos de entrada e chaves fornecidos.

2.2.3. Impressão dos Resultados

Após a chamada da função idea round, o programa entra em um loop que: Carrega os resultados do bloco de saída. Prepara argumentos para a chamada de sistema write para imprimir os resultados no console. Realiza a chamada de sistema write para imprimir os resultados. Avança para o próximo elemento no bloco de saída. Verifica se o loop deve continuar.

2.2.4. idea-round:

Esta função implementa uma rodada da operação IDEA, que é um algoritmo de criptografia simétrica. Ela recebe argumentos da função main e realiza as seguintes etapas: Realiza uma multiplicação condicional (mul) entre dois argumentos. Realiza várias operações de permutação e substituição de acordo com o algoritmo IDEA. Armazena os resultados de volta no bloco de saída. O código implementa uma única rodada do algoritmo IDEA e imprime os resultados no console. Lembre-se de que o algoritmo IDEA é mais complexo e normalmente envolve várias rodadas para criptografar ou descriptografar dados. Este código parece ser uma implementação simplificada de uma rodada apenas para fins de demonstração.

Referências