Universidade de Brasília – UnB
Instituto de Ciências Exatas – IE
Departamento de Ciência da Computação – CIC
CIC0201 - Segurança da Computação - 2023/2
Professora: João Gondim
Aluno: João Vitor Abadio Siqueira

Descritivo - Trabalho de Implementação 3 - Gerador/Verificador de Assinaturas

Para compilar o programa:

Compile: gcc rsa.c -lgmp -lcrypto -o rsa

Para executar:

./rsa

Como o programa funciona

O programa implementa a cifra RSA. Ao executar o programa um menu será exibido com as opções de cifração/decifração e assinatura/verificação.

int miller_rabin_pass(mpz_t a, mpz_t n):

A função realiza o algoritmo de Miller-Rabin, retornando 1 caso o número seja provavelmente primo e 0 caso seja composite.

int miller_rabin(mpz_t n, gmp_randstate_t rand_state):

É a função que irá gerar o número aleatório e chamar a **miller_rabin_pass** vinte vezes para ter maior garantia da primalidade.

void key_generation(mpz_t e, mpz_t d, mpz_t n, gmp_randstate_t state):

Inicia com p e q provavelmente primos e realiza todos os passos para a geração de chaves. Eu vou deixar um .jpg (ou .png) no git com o algoritmo descrito no livro do Stallings para facilitar o entendimento da nomenclatura que usei.

void rsa_encrypt(const mpz_t n, const mpz_t e, const mpz_t m, mpz_t c)
void rsa_decrypt(const mpz_t n, const mpz_t d, const mpz_t c, mpz_t m):

Realizam a criptografia e descriptografia de inteiros em rsa usando exponenciação modular.

void handleErrors(void)):

Lida com erros que podem ocorrer na próxima função

void digest_message(const unsigned char *message, size_t message_len, unsigned char **digest, unsigned int *digest_len)

Função “pronta” que é usada como interface para hashes pelo OpenSSL, é só substituir o EVP_sha3_256() pelo hash que quiser usar.

int compare_hash(const unsigned char* hash1, const unsigned char* hash2)

Compara o tamanho e cada caractere de dois hashes.

int main():

Gera o estado aleatório requerido pela GMP, inicializa as chaves e variáveis para mensagem, mensagem cifrada.

Gera a chave.

Exibe menu com 3 opções:

- Cifracao/Decifracao assimetrica de inteiros
- Assinatura/Verificacao RSA de strings
- Sair