SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
PRÓ-REITORIA DE GRADUAÇÃO
Rodovia SC 484, km 02, Fronteira Sul, Chapecó-SC, CEP 89815-899, 49 2049-3710
www.uffs.edu.br

Trabalho 2 – Implementação do RSA

Componente Curricular: GEX112 - Segurança e auditoria de sistemas		
Créditos: 4	Número da turma: 32517	Ano/semestre: 2021.2
Curso(s)/fase de oferta:	1100 - CIÊNCIA DA COMPUTAÇÃO / 0ª fase (Optativa) 1101 - CIÊNCIA DA COMPUTAÇÃO / 9ª fase	
Professor(es): Felipe Grando E-mail de contato: felipegrando@uffs.edu.br		

1. Descrição

Trabalho **individual** de implementação do algoritmo RSA em **Python**.

O algoritmo deve possuir 3 funcionalidades:

1) **Criar Chaves:** solicitar ao usuário que seja informado dois números primos para a criação das chaves pública e privada do RSA. Realizar os cálculos necessários e imprimir em tela a chave pública e a chave privada geradas.
2) **Cifrar Mensagem:** solicitar ao usuário a chave pública que será utilizada e o nome do arquivo com a mensagem a ser criptografada (adotar como padrão que o arquivo está localizado na mesma pasta do código do programa). Transformar o texto plano do arquivo numa codificação numérica (use a codificação da Figura 1), criptografar a mensagem e salvar o resultado em um novo arquivo texto.
3) **Decifrar Mensagem:** solicitar ao usuário a sua chave privada e o nome do arquivo com a mensagem a ser decifrada (adotar como padrão que o arquivo está localizado na mesma pasta do código do programa). Transformar o texto criptografado do arquivo em texto plano novamente (decodificando os números em letras) e apresentar em tela para o usuário.

1	2	3	4	5	6	7	8	9	10	11
A	B	C	D	E	F	G	H	I	J	L

12	13	14	15	16	17	18	19	20	21	22	23
M	N	O	P	Q	R	S	T	U	V	X	Z

Figura 1 - Codificação Numérica das Letras

Observações:

a) O algoritmo pode usar qualquer critério para a escolha do valor de ***e***, no entanto, atente-se para as restrições ($1 < e < \varphi(n)$; $MDC(\varphi(n), e) = 1$).
b) O algoritmo não precisa funcionar para valores de primos muito grandes (estes podem ocasionar problemas numéricos nos cálculos, exigindo cuidados específicos na implementação).
c) A implementação do algoritmo não pode utilizar bibliotecas que já implementem o RSA, mas bibliotecas auxiliares para facilitar os cálculos podem ser utilizadas livremente.

2. Método de Avaliação

A avaliação do trabalho considerará os seguintes itens: corretude da implementação, organização e documentação do código.

A realização e entrega deste trabalho no Moodle até a data prevista (10/02/2022) contará como 4 presenças no dia 16/12 (aula assíncrona) e valerá uma nota de 0 a 10 que comporá 15% da nota final do CCR.

Será dado nota 0 (zero) e 4 faltas no dia 16/12 para todos os alunos que não entregarem o trabalho dentro do prazo estipulado ou que plagiarem o trabalho de um colega.
O aluno poderá, se desejar, recuperar a nota do trabalho (corrigindo os pontos falhos) se entregá-lo novamente até a data 24/02/2022. A nota final no trabalho será a média das duas notas. Isso vale também para quem entregar o trabalho atrasado, nesse caso a média será entre 0 (da primeira entrega não realizada) e a nota da segunda entrega.

3. Material de Apoio

Consultar os slides disponibilizados no Moodle para a aula do dia 16/12/2021.