

## **ROTEIRO LAB – COMUNICAÇÃO PRIVADA**

**OBJETIVO:** DEMONSTRAR NA PRÁTICA EFEITOS DE PRIVACIDADE NA INTERNET. PARTA TANTO O ALUNO DEVERÁ SE COMUNICAR DE MANEIRA CIFRADA UTILIZANDO MECANISMOS DE CORREIO ELETRONICO INSEGUROS.

**RESULTADO ESPERADO:** AO FINAL DO LABORATÓRIO, O ALUNO DEVERÁ SER CAPAZ DE ENTENDER OS CONCEITOS PRÁTICOS DE CHAVES PÚBLICAS E PRIVADAS E COMO SE DÁ O PROCESSO DE ENCRIPTAÇÃO/DECRIPTAÇÃO DE MENSAGENS.

**SIGA OS SEGUINTE PASSOS USANDO O NAVEGADOR FIREFOX.**

**ATENÇÃO: SÓ PASSE PARA O PASSO SEGUINTE APÓS A CONCLUSÃO DO PASSO EM QUE SE ENCONTRA.**

**PASSOS:**

1 – ACESSE O SITE [WWW.GMAIL.COM](http://WWW.GMAIL.COM) E CRIE UMA CONTA DE USUÁRIO PARA FINS DE TESTAR A COMUNICAÇÃO PRIVADA POR CANAIS INSEGUROS.

NOME DA CONTA CRIADA: \_\_\_\_\_

ANOTE A SENHA DA CONTA CRIADA: \_\_\_\_\_

2 – TENHA CERTEZA QUE A CONTA ESTÁ FUNCIONAL. PARA TANTO, SOLICITE PARA DOIS COLEGAS DE SALA AS RESPECTIVAS CONTAS CRIADAS.

CONTA DE MAIL DO COLEGA 1: \_\_\_\_\_

CONTA DE MAIL DO COLEGA 2: \_\_\_\_\_

3 – ENVIE UM MAIL DA SUA CONTA CRIADA PARA CADA UM DOS COLEGAS E VERIFIQUE SE CADA UM RECEBEU A INFORMAÇÃO CORRESPONDENTE ENVIADA POR VOCÊ.

4 – ABRA O NAVEGADOR FIREFOX (OU O GOOGLE CHROME) E ACESSE O ENDEREÇO [WWW.MAILVELOPE.COM](http://WWW.MAILVELOPE.COM)

5 – LOCALIZE O PLUGIN PARA O FIREFOX E FAÇA O DOWNLOAD

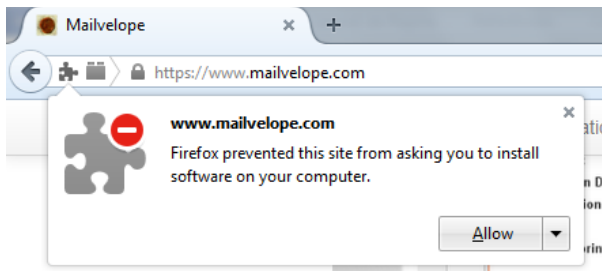
### **Firefox Addon**

A Firefox version of Mailvelope is available at  
[download.mailvelope.com](http://download.mailvelope.com).

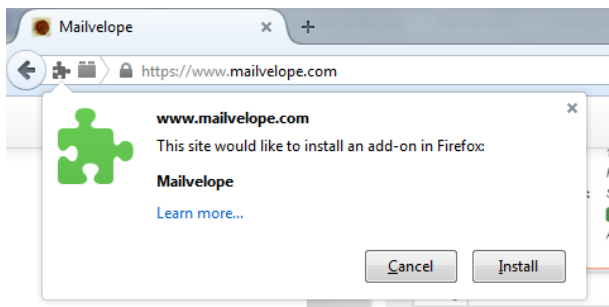


**Firefox**

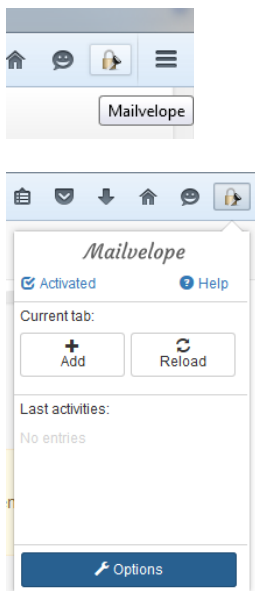
6 – PERMITA QUE O PLUGIN SEJA INSTALADO CLICANDO EM **ALLOW/PERMITIR**.



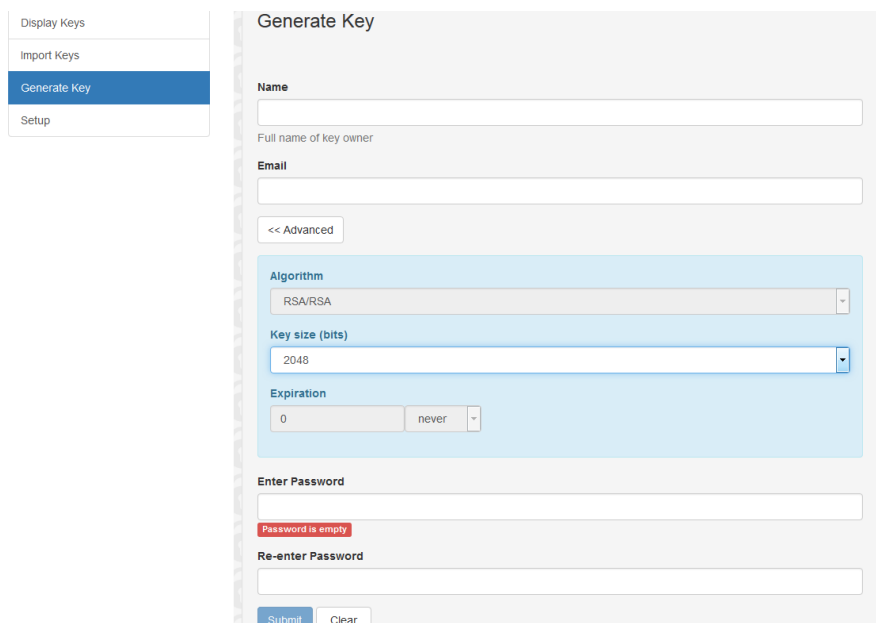
7 – CLIQUE EM **INSTALL/INSTALAR**



8 – LOCALIZE O NOVO ÍCONE CRIADO NA BARRA DE MENUS/NAVEGAÇÃO E CLIQUE NO CADEADO E A SEGUIR EM **OPTIONS**



9 – CLIQUE EM **GENERATE KEYS** E PREENCHA OS CAMPOS CONFORME EXPLICADO A SEGUIR:



10 – NOS RESPECTIVOS CAMPOS:

**NAME:** PREENCHA COM SEU NOME

**MAIL:** O EMAIL CRIADO NO PASSO 1.

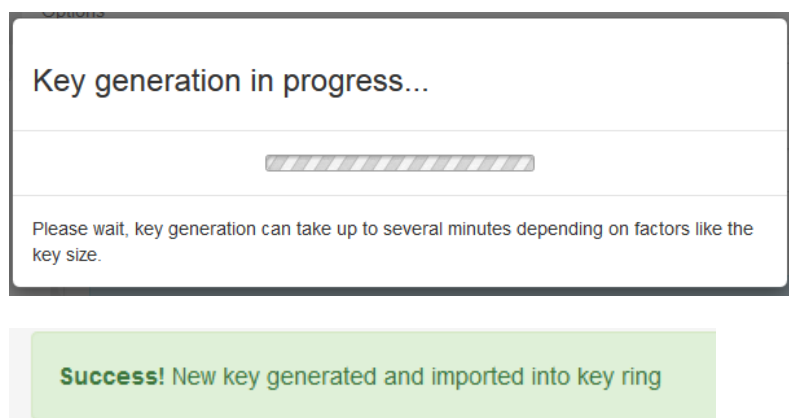
CLIQUE NO BOTÃO **ADVANCED** E ESCOLHA A OPÇÃO DE **KEY SIZE** COM 2048

CRIE UMA SENHA E A DIGITE DUAS VEZES

ANOTE A SENHA CRIADA: \_\_\_\_\_

CLIQUE EM **SUBMIT**

11 – AGUARDE O PROCESSO DE GERAÇÃO CONCLUIR



12 – VISUALIZE A SUA CHAVE GERADA CLICANDO NA OPÇÃO **DISPLAY KEYS**.

13 – CLIQUE NA SUA CHAVE UMA VEZ E VISUALIZE OS DETALHES

## Key Details



Main Key

Subkeys

User IDs

Export

Name

ALUNO

Email

teste@gmail.com

Key ID

BE77C2A30F6D0E10

Algorithm

RSA (Encrypt or Sign)

Length

2048

Creation Date

2015-10-15

Expiration Date

The key does not expire

Fingerprint

B0DC 4FA1 F5B4 EAD1 85E2 7E22 BE77 C2A3 0F6D 0E10

Status

valid

Type



Key Pair

14 – CLIQUE EM **CLOSE**.

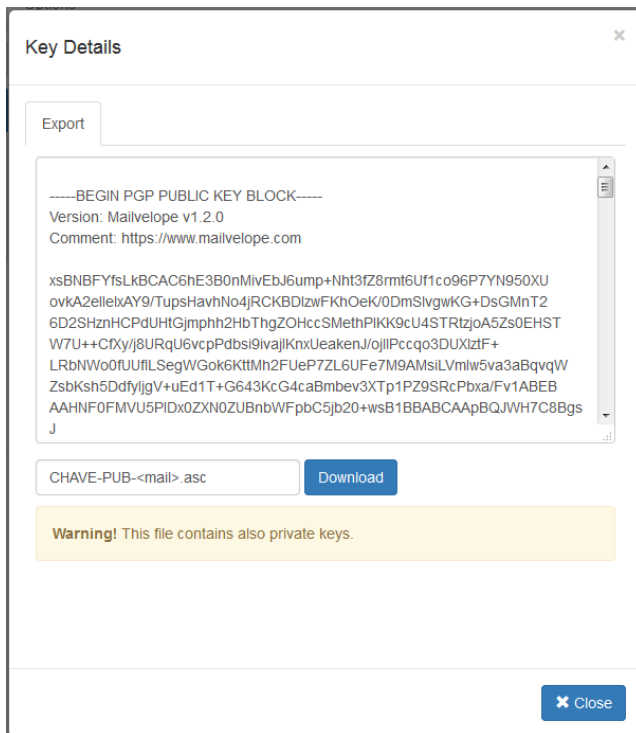
15 – MINIMIZE O NAVEGADOR. ABRA O WINDOWS EXPLORER.

NO WINDOWS EXPLORER, CRIE UMA NOVA PASTA EM SEUS DOCUMENTOS CHAMADA **CHAVES-LAB**



16 – VOLTE AO NAVEGADOR E CLIQUE NO BOTÃO **EXPORT**

Export		Key type		
		All		
Name	Email	Key ID	Created	
ALUNO <span>Primary</span>	teste@gmail.com	BE77C2A30F6D0E10	2015-10-15	



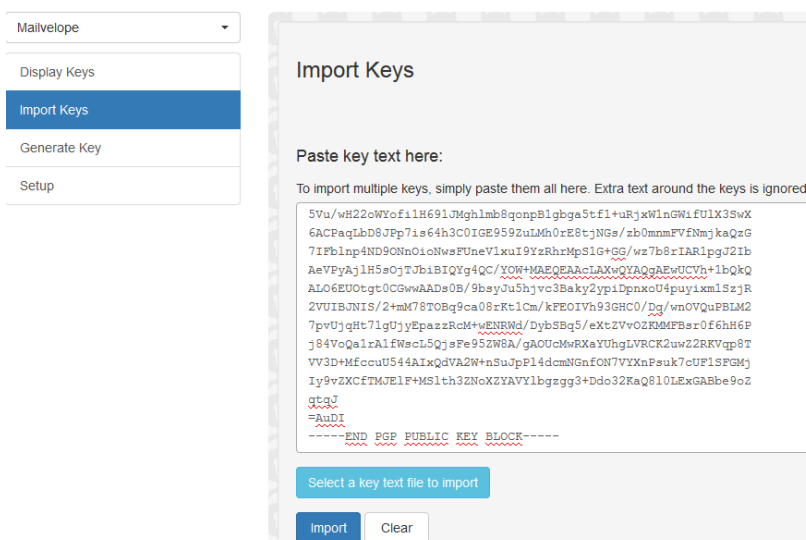
17 – ESCOLHA A CHAVE PUBLICA PARA EXPORTAÇÃO E COLOQUE O NOME DO ARQUIVO COMO: **CHAVE-PUB<MAIL>.ASC**, sendo que **<MAIL>** É O NOME DA CONTA DE EMAIL CRIADA NO PASSO 1. A SEGUIR CLIQUE EM DOWNLOAD.

18 – LOCALIZE O ARQUIVO NA SUA PASTA DOWNLOADS E O TRANSFIRA PARA A PASTA **CHAVES-LAB**, CRIADA NO PASSO 15.

19 – SOLICITE AOS DOIS COLEGAS DO PASSO 2 QUE TE ENVIEM O ARQUIVO CHAVE-PUB<MAIL>.ASC COMO ANEXO DO MAIL CRIADO POR CADA UM DELES.

20 – ABRA O SEU MAIL DO GMAIL CRIADO NO PASSO 1 E FAÇA O DOWNLOAD DE CADA ARQUIVO RECEBIDO E O COLOQUE NA PASTA CRIADA NO PASSO 15.

21 – DE VOLTA AS OPÇÕES DO MAILVELOPE, CLIQUE NA OPÇÃO **IMPORT KEYS**. NA JANELA, CLIQUE EM **SELECT A KEY TEXT FILE TO IMPORT**. A SEGUIR SELECIONE UM ARQUIVO PARA IMPORTAR, CONFIRME A OPERAÇÃO E CLIQUE EM **IMPORT**.



Success! Public key 00B3BA1143AD82DD of user TESTE2 <ALUNO2@GMAIL.COM> imported into key ring

23 – APÓS IMPORTAR A PRIMEIRA CHAVE, CLIQUE EM **IMPORT ANOTHER**. REPITA A OPERAÇÃO PARA O SEGUNDO ARQUIVO. TENHA CERTEZA DO SUCESSO DA IMPORTAÇÃO DAS DUAS CHAVES.

22 – CLIQUE NA OPÇÃO **DISPLAY KEYS** E VERIFIQUE OS DETALHES DE CADA CHAVE IMPORTADA. VOCÊ DEVERÁ TER 3 CHAVES. SENDO QUE A SUA É A PRIMÁRIA E COMPLETA (POSSUI A CHAVE PÚBLICA E A CHAVE PRIVADA). NO CASO DOS DEMAIS, DEVE POSSUIR A CHAVE PÚBLICA DE CADA UM.

Display Keys

Import Keys

Generate Key

Setup

Key Management

Export

Key type All

Name	Email	Key ID	Created
ALUNO <span>Primary</span>	teste@gmail.com	BE77C2A30F6D0E10	2015-10-15
ALUNO3	TESTE3@GMAIL.COM	CC920783B02C5CAB	2015-10-15
TESTE2	ALUNO2@GMAIL.COM	00B3BA1143AD82DD	2015-10-15

23 – ABRA A PÁGINA DO GMAIL.COM COM A CONTA CRIADA NO PASSO 1. GERE UM NOVO MAIL PARA UM DOS DESTINATÁRIOS QUE POSSUI A CHAVE PÚBLICA. SENDO QUE:

**PARA:** DESTINO QUE JÁ TEM O MAIL.COM CHAVE PUBLICA

**DE:** A SUA PROPRIA CONTA ;

Mensaje nuevo

Para

De

Cc Cco

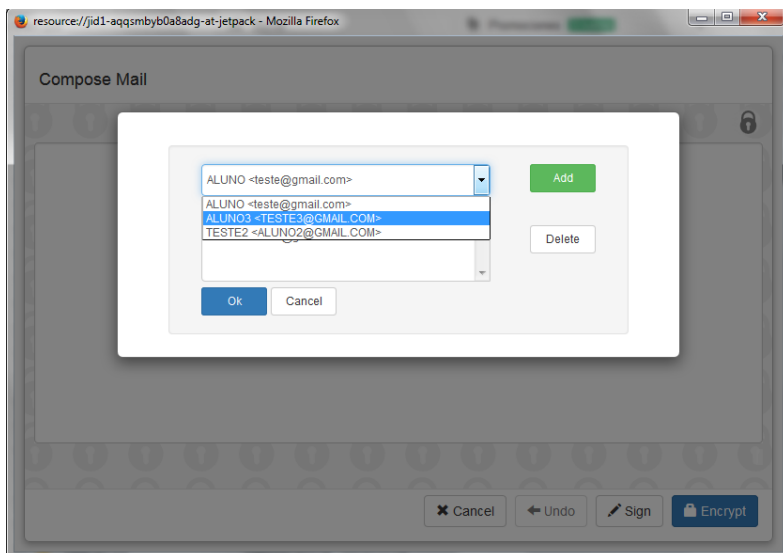
Asunto

--

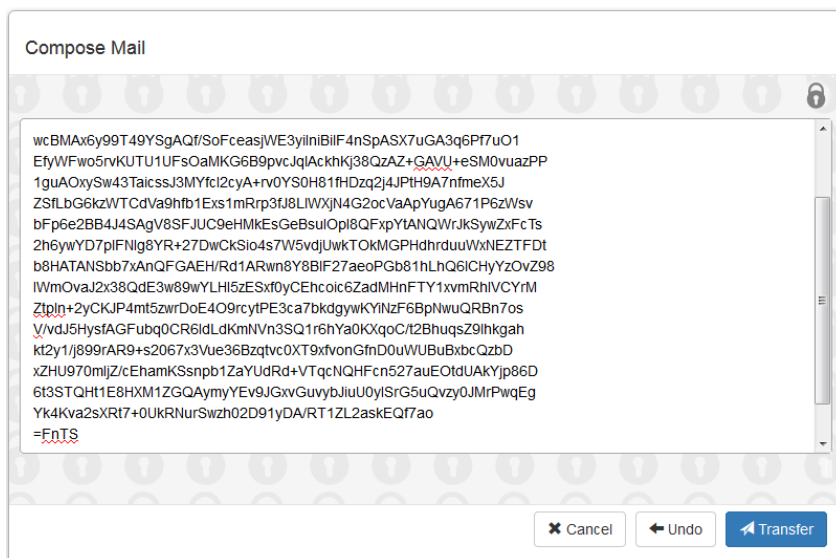
PERCEBA NA JANELA UM ÍCONE DE UM PAPEL COM LAPIS E CLIQUE SOBRE ELE. IRÁ ABRIR A JANELA DO MAILVELOPE DE CRIAÇÃO DE MAIL.

24 – NA JANELA QUE SE ABRE, DIGITE UMA MENSAGEM QUALQUER PARA O SEU DESTINATÁRIO.

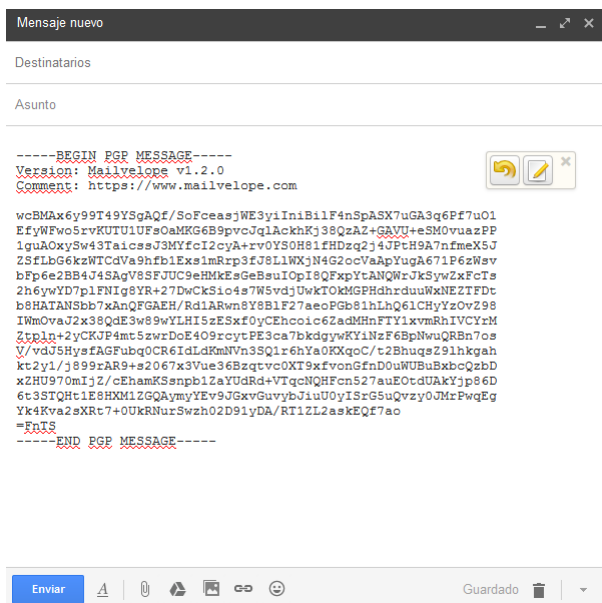
25 – CLIQUE NO BOTÃO **ENCRYPT**. A SEGUIR ESCOLHA O DESTINO QUE TEM A CHAVE PUBLICA CORRESPONDENTE E CLIQUE **ADD** E DEPOIS **OK**.



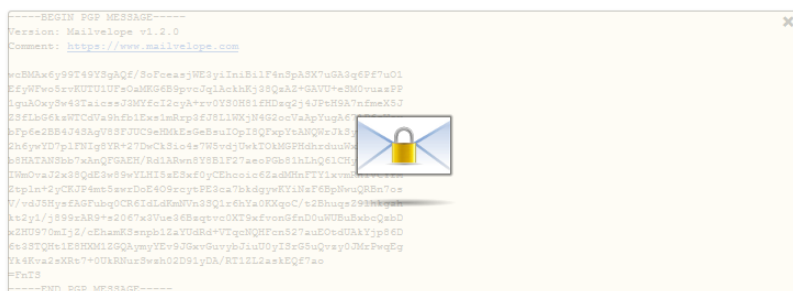
26 – NA JANELA DE COMPOSE MAIL, VERIFIQUE COMO FICOU A NOVA MENSAGEM. CLIQUE EM **TRANSFER**.



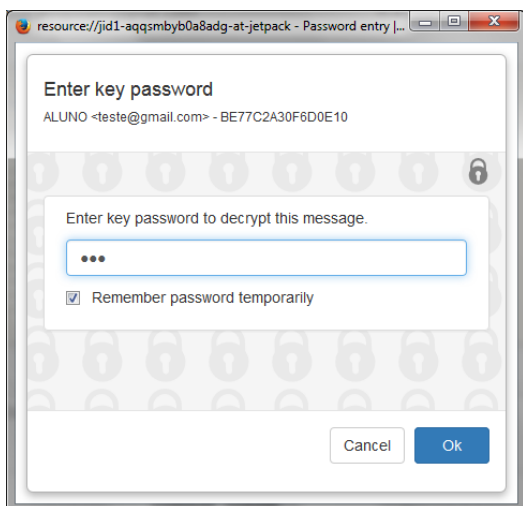
27 – TENHA CERTEZA DOS DESTINATÁRIOS. SE DESEJAR, COLOQUE UM ASSUNTO NA MENSAGEM E CLIQUE EM **ENVIAR**.



28 – VERIFIQUE COM O SEU COLEGA QUE ENVIOU A MENSAGEM PARA VOCÊ SE ELE JÁ COMPLETOU O PROCEDIMENTO CORRESPONDENTE. A SEGUIR VERIFIQUE COMO FICOU A SUA CAIXA DE ENTRADA NO GMAIL. AO RECEBER UM NOVO MAIL ENCRIPTADO, O APLICATIVO IRÁ MARCÁ-LO COM UM ENVELOPE CONFORME A IMAGEM ABAIXO.

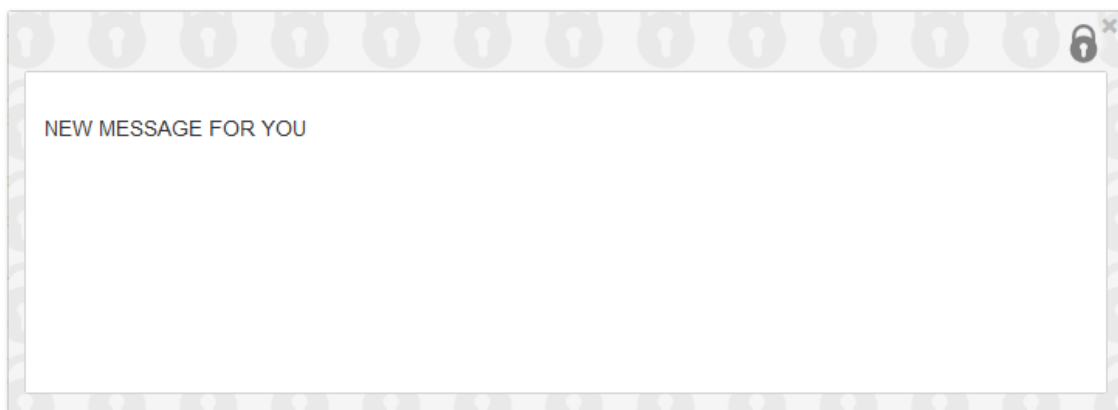


29 - CLIQUE NO ENVELOPE E DIGITE A SENHA CRIADA NO PASSO 10 E CLIQUE **OK**



VOCÊ DEVERÁ SER CAPAZ DE VER A SUA MENSAGEM DECIFRADA NA JANELA DO NAVEGADOR.





**30 – REPITA OS PASSOS DE ENVIAR UM NOVO EMAIL ENCRYPTADO PARA QUALQUER UM DOS COLEGAS QUE VOCÊ NÃO TENHA A CHAVE PÚBLICA. DESCREVA O QUE ACONTECEU AO SE RECEBER UMA MENSAGEM QUE O DESTINATÁRIO NÃO TENHA A CHAVE PÚBLICA.**


**31 – PARA FINS DE DEMONSTRAÇÃO, PASSE PARA O SEU COLEGA DO LADO, A CONTA DE EMAIL E SENHA CRIADO NO PASSO 1. VERIFIQUE SE ELE CONSEGUE VERIFICAR O CONTEÚDO DAS MENSAGENS ENCRYPTADAS SEM AS RESPECTIVAS CHAVES DO PASSO 10.**