

Trabalho PGP

Aluna: Jessica Regina dos Santos

Disciplina: Segurança da Computação

Data de Entrega: 19/05/25

Questão 1)

Utilizei o software Kleopatra para gerar um par de chaves. Em seguida, minha chave pública foi publicada em um servidor público. A publicação foi realizada em <https://keyserver.ubuntu.com>. A chave pode ser localizada publicamente através do meu e-mail, que está vinculado, ou da KEY ID.

Search results for 'jessicars241@gmail.com'

Type	bits/keyID	cr. time	exp time	key expir
pub	(4)eddsa263/75a43496fe606e5b6065a988f494af6db734a9ce	2025-05-15T22:12:00Z		
uid	Jessica_Regina_dos_Santos_<jessicars241@gmail.com>			
sig	cert	f494af6db734a9ce	2025-05-15T22:12:00Z	2028-05-15T15:00:00Z [selfsig]
sub	(4)ecdh263/18dc64036a7e7ec4c62010be2a6272b06d7e3be0	2025-05-15T22:12:00Z		
sig	sbind	f494af6db734a9ce	2025-05-15T22:12:00Z	2028-05-15T15:00:00Z []

Imagem 1. Chave publicada para a questão 1. KEY ID: F494 AF6D B734 A9CE.

Questão 2)

Revoguei minha chave PGP por meio do software Kleopatra, uma interface gráfica para o gerenciamento de certificados. Realizei o experimento em um sistema Windows 10 e adotei como servidor de chaves públicas o repositório OpenPGP Keyserver.

Utilizando o Kleopatra, criei um novo par de chaves. Foram preenchidos os campos com o meu nome completo e meu e-mail. Utilizei a curva elíptica “ed25519” como algoritmo de criptografia (há a possibilidade de escolher outros algoritmos, como o RSA, que aprendemos em sala). Em seguida, criei a senha para proteger minha chave, que foi gerada com sucesso. Foi realizado o backup da minha chave privada no meu computador.

Concluída a criação do par de chaves, procedeu-se a publicação no servidor público utilizando diretamente a interface principal do Kleopatra, clicando sobre o certificado criado e selecionando “Publicar no Servidor”. Assim, a chave foi enviada ao repositório público keyserver.ubuntu.com. Em seguida, foi possível verificar a publicação realizando uma busca direta pelo meu endereço de e-mail (jessicars241@gmail.com) no site do servidor. A chave está listada com suas informações e status válido, como abaixo:

Search results for 'jessicars241@gmail.com'

Type	bits/keyID	cr. time	exp time	key expir
pub	(4)eddsa263/18651e4d8d428e5164f4327fb672ae864a448bb1	2025-05-15T22:40:42Z		
uid	Jessica Regina dos Santos <jessicars241@gmail.com>			
sig	cert	b672ae864a448bb1	2025-05-15T22:40:42Z	2028-05-15T15:00:00Z [selfsig]
sub	(4)ecdh263/756d209feb2f22df1fb94ba2bfa789b399d12397	2025-05-15T22:40:42Z		
sig	sbind	b672ae864a448bb1	2025-05-15T22:40:42Z	2028-05-15T15:00:00Z []

pub	(4)eddsa263/75a43496fe606e5b6065a988f494af6db734a9ce	2025-05-15T22:12:00Z		
uid	Jessica Regina dos Santos <jessicars241@gmail.com>			
sig	cert	f494af6db734a9ce	2025-05-15T22:12:00Z	2028-05-15T15:00:00Z [selfsig]
sub	(4)ecdh263/18dc64036a7e7ec4c62010be2a6272b06d7e3be0	2025-05-15T22:12:00Z		
sig	sbind	f494af6db734a9ce	2025-05-15T22:12:00Z	2028-05-15T15:00:00Z []

Imagem 2. Minha segunda chave (KEY ID: B672 AE86 4A44 8BB1) criada para a questão 2.

É importante destacar que o repositório não sobrescreve chaves existentes (como a maioria dos servidores compatíveis com o protocolo OpenPGP). Assim, várias chaves podem coexistir associadas a um único e-mail (Koch et al., 2023). Também é importante destacar a necessidade de sempre estar atualizando a página da Imagem 2 (atualização do conteúdo do servidor).

Em seguida, a chave foi revogada. O processo de revogação também ocorreu utilizando o Kleopatra, por meio da opção “Revogar Certificado”. A revogação foi confirmada e passou a constar visualmente no Kleopatra com o status apropriado. O certificado foi novamente exportado ao servidor público.

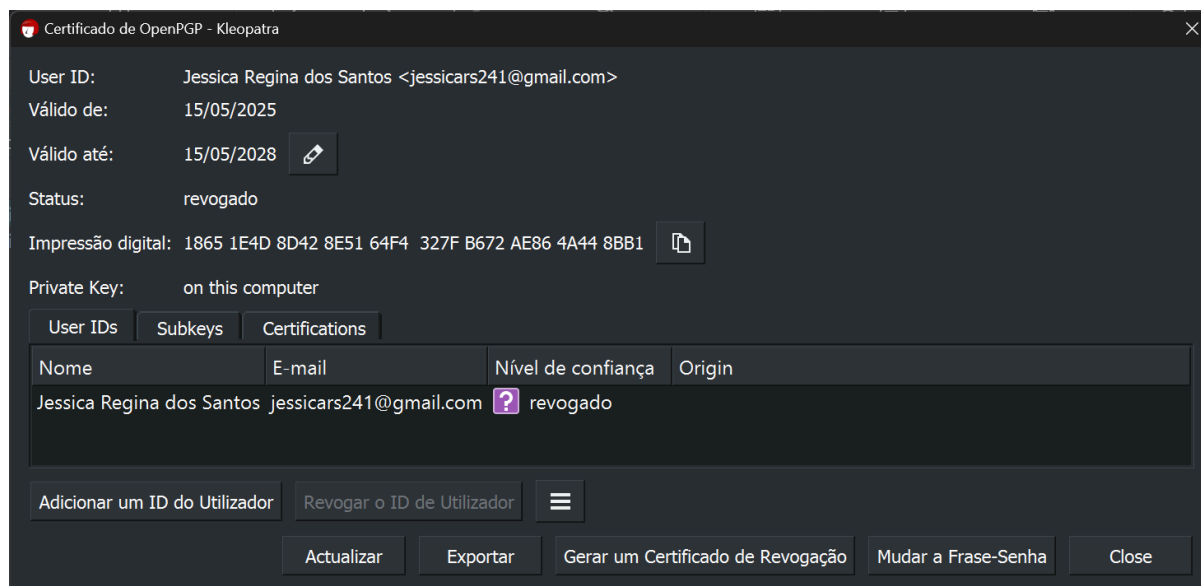


Imagem 3. Revogação confirmada no Kleopatra.

Search results for '0xB672AE864A448BB1'

Type	bits/keyID	cr. time	exp time	key expir
pub	(4)eddsa263/18651e4d8d428e5164f4327fb672ae864a448bb1	2025-05-15T22:40:42Z		
sig	revok b672ae864a448bb1	2025-05-15T22:56:50Z		[selfsig]
sub	(4)ecdh263/756d209feb2f22df1fb94ba2bfa789b399d12397	2025-05-15T22:40:42Z		
sig	sbind b672ae864a448bb1	2025-05-15T22:40:42Z		2028-05-15T15:00:00Z []

Imagem 4. Revogação confirmada no servidor público.

Nesse exercício, foi possível compreender o ciclo de vida de um par de chaves PGP, desde sua criação local até a publicação e revogação. O processo se mostrou bastante acessível utilizando a interface gráfica do Kleopatra.

Questão 3)

Para Segurança da Computação, assinar digitalmente o certificado de outra pessoa equivale a certificá-lo, ou seja, estou atestando com a minha chave privada que acredito que a chave pública daquela pessoa realmente pertence à identidade informada (Zimmermann, 1995; GNU Privacy Handbook, 2001).

Utilizando o Kleopatra, realizei a certificação. Para isso, importei o certificado da minha colega Myllena e utilizei a minha chave privada para gerar a assinatura. Após a certificação, enviei a chave assinada ao servidor para que ficasse publicamente visível

Informações da assinatura:

Search results for 'correameyllena048@gmail.com'

Type	bits/keyID	cr. time	exp time	key expir
pub	(4)rsa4096/25612462198c736287d63ea962ce23a44f0c1c97	2025-05-17T14:06:22Z		
uid	Myllena da Conceição Corrêa <correameyllena048@gmail.com>			
sig	cert 62ce23a44f0c1c97	2025-05-17T14:06:22Z	2028-05-17T15:00:00Z	[selfsig]
sig	cert 1053bc26d482f18e	2025-05-17T17:22:55Z		1053bc26d482f18e
sub	(4)rsa4096/8c59b063ecfb15fcb02b50501c03e1675357ab57	2025-05-17T14:06:22Z		
sig	sbind 62ce23a44f0c1c97	2025-05-17T14:06:22Z		2028-05-17T15:00:00Z []

Imagem 5. Informações da assinatura.

- Key ID da chave assinada: 62CE 23A4 4F0C 1C97
- Key ID da minha assinatura: 1053 BC26 D482 F18E
- Data da assinatura: 17/05/25
- Status (após upload ao servidor): chave com assinatura de terceiro visível no servidor.

Logo, a assinatura foi realizada com sucesso! O identificador da minha assinatura aparece como um tipo “sig cert” associado à identidade da minha colega, refletindo a confiança estabelecida entre nossas identidades digitais. Esse processo faz parte da construção da chamada Rede de Confiança, onde a confiança entre usuários é descentralizada e estabelecida com base na verificação mútua de identidades (Zimmermann, 1995).

Em seguida, revoguei minha assinatura. O processo de revogação também ocorreu utilizando o Kleopatra, por meio da opção “Revogar Certificado”. A revogação foi confirmada e passou a constar visualmente no Kleopatra com o status apropriado. Em seguida, foi realizada a exportação para o servidor público.

Search results for '0x1053BC26D482F18E'

Type	bits/keyID	cr.	time	exp	time	key	expir
pub	(4)eddsa263/a46ed9bf0e62da423b8353511053bc26d482f18e						2025-05-16T14:05:57Z
sig	revok	1053bc26d482f18e					2025-05-18T14:04:33Z [selfsig]
sub	(4)ecdh263/c531184482236ab3c5e04a2b5c970293d7c45092						2025-05-16T14:05:57Z
sig	sbind	1053bc26d482f18e					2025-05-16T14:05:57Z 2028-05-16T15:00:00Z []

Imagem 6. Minha assinatura foi revogada.

Questão 4) O que é o anel de chaves privadas? Como este está estruturado? Na sua aplicação PGP onde este anel de chaves é armazenado? Quem pode ser acesso a esse porta chaves?

O anel de chaves privadas é uma estrutura utilizada por aplicações de criptografia para armazenar com segurança os pares de chaves privadas pertencentes ao usuário. Essas chaves são muito importantes para operações como assinatura digital e descriptografia de mensagens (Callas et al., 2007).

A estrutura do anel de chaves é composta por arquivos criptografados. Tais armazenam a chave privada em si e metadados, como: identificador da chave (Key ID), fingerprint, datas de criação e validade, identificadores do usuário (nome completo, e-mail), entre outros. Também estão incluídas subchaves, informações relacionadas à revogação e status. Essas chaves são protegidas por algoritmos criptográficos e são desbloqueadas fornecendo uma senha criada pelo usuário anteriormente (GnuPG, 2023).

No caso específico do meu sistema operacional Windows, ao utilizar o Kleopatra, minhas chaves privadas são armazenadas em uma pasta padrão no meu computador. Essa pasta contém arquivos binários criptografados, não legíveis diretamente. As chaves públicas correspondentes são mantidas em arquivos destinados às mesmas (Gpg4win, 2023).

O acesso ao anel de chaves privadas é restrito ao usuário do sistema que as criou (no caso eu, a estudante). Mesmo que algum outro usuário obtivesse acesso ao diretório onde

estão os arquivos, não seria possível utilizá-los sem conhecer a senha das chaves privadas (GnuPG, 2023).

Questão 5) Qual a diferença entre assinar uma chave local e assinar no servidor?

No contexto do PGP, assinar uma chave significa declarar que se confia na correspondência entre a chave pública e a identidade do seu proprietário. Porém, existem diferenças entre assinar uma chave localmente e publicar esta assinatura em um servidor de chaves.

Quando assinamos uma chave localmente, a assinatura permanece armazenada apenas no nosso sistema – o usuário que realizou a assinatura. Trata-se de uma declaração de confiança privada, utilizada apenas pelo próprio sistema para verificar a autenticidade de mensagens ou certificados assinados por aquela chave. Essa assinatura não é exportada para terceiros, nem está visível para outros usuários. A prática é comum em ambientes de uso pessoal, quando não há a intenção de construir uma rede pública de confiança (GnuPG, 2023).

Já, ao assinar uma chave e publicar a assinatura em um servidor de chaves público (como o keyserver.ubuntu.com) essa assinatura se torna visível para qualquer usuário interessado em consultar a chave. Essa ação faz parte do modelo de confiança descentralizado conhecido como Rede de Confiança, onde os usuários confiam nas validações feitas por terceiros para decidir se devem aceitar uma chave como autêntica (Callas et al., 2007). A assinatura publicada reflete publicamente a confiança do assinante naquela identidade, e pode ser usada por outras pessoas.

Assim, a principal está no alcance de confiança atribuída. Localmente é restrito ao próprio usuário e no servidor de chaves é compartilhado com a comunidade.

Questão 6) O que é e como é organizado o banco de dados de confiabilidade?

O banco de dados de confiabilidade é uma estrutura mantida localmente pela aplicação de criptografia (como o GnuPG ou o Kleopatra) que registra o nível de confiança atribuído às chaves públicas e aos seus respectivos donos. Tal não armazena diretamente o conteúdo das chaves, e sim informações sobre quais chaves o usuário considera válidas e confiáveis (GnuPG, 2023).

O banco é organizado seguindo o modelo descentralizado da Rede de Confiança, onde a verificação da identidade de uma chave pública é feita por meio da assinatura de terceiros. Assim, quanto mais pessoas confiáveis assinarem uma chave, mais confiável ela será considerada (Callas et al., 2007).

Duas informações principais ficam mantidas no banco: *Trust Owner* – indica quanto o usuário confia que o proprietário de uma chave é capaz de assinar corretamente outras chaves. *Validade* – indica quanto o sistema pode confiar que a chave realmente pertence à identidade informada. Esse valor é com base nas assinaturas recebidas e nos níveis de confiança atribuídos aos assinantes (Gpg4win, 2023).

O banco de dados de confiabilidade é essencial para que o sistema determine se uma chave pública é considerada segura para uso. Ele permite alertar o usuário caso alguma chave não tenha validade suficiente, evitando ataques e uso de chaves falsas (Callas et al., 2007).

Questão 7) O que são e para que servem as sub-chaves?

Sub-chaves são chaves associadas a uma chave principal e são utilizadas para distribuir funções criptográficas específicas, como assinatura, criptografia ou autenticação, sem comprometer a chave principal. Também podem operar de maneira independente dentro dos limites autorizados pela chave principal (Callas et al., 2007).

A utilização de sub-chaves também tem como objetivo aumentar a segurança operacional. Enquanto a chave primária é geralmente usada para assinar outras chaves e manter a identidade do usuário, as sub-chaves podem ser utilizadas no dia a dia para tarefas comuns, já citadas. Desta forma, a chave principal pode ser mantida em um ambiente seguro (como um ambiente offline), enquanto apenas as sub-chaves ficam acessíveis em dispositivos utilizados rotineiramente (GnuPG, 2023). Este comportamento reduz os riscos de compartilhamento da chave principal, crítica para a identidade digital do usuário.

Cada subchave geralmente tem um identificador único (um propósito) e data de expiração configurável. Uma chave PGP pode conter uma chave primária e uma ou mais sub-chaves com funções específicas. No Kleopatra, ao criar um novo par de chave, as sub-chaves são geradas automaticamente, mantendo a chave primária como certificadora. As sub-chaves aparecem listados abaixo da chave principal com suas respectivas funções, fingerprint, algoritmo, etc.

Questão 8) Coloque sua foto (ou uma figura qualquer) que represente você em seu certificado PGP.

Passo a passo de como eu adicionei uma foto a minha chave PGP usando GPG:

1. Listando minhas chaves no anel de chaves: `gpg --list-keys`

Esse comando exibe todas as chaves públicas armazenadas no meu anel de chaves. Verifiquei que possuo três chaves associadas ao meu e-mail, sendo que duas estão revogadas e uma está ativa (plena).

2. Editando a chave ativa: `gpg --edit-key 75A43496FE606E5B6065A988F494AF6DB734A9CE`

Esse comando abre um modo para editar essa chave específica (fingerprint).

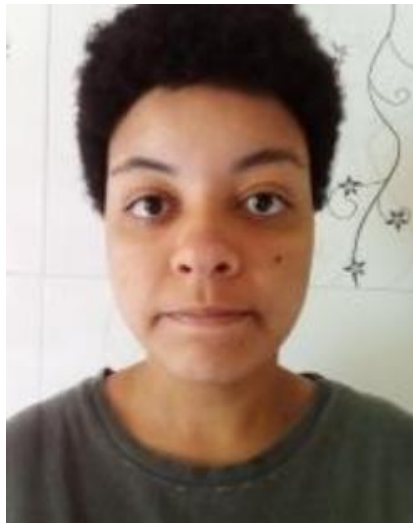
3. Adicionando uma foto (ID fotográfica): `addphoto`

Esse comando permite anexar uma imagem JPEG à minha chave. Essa imagem é embutida à minha chave pública.

4. Informe o caminho da imagem no meu computador.
5. O GPG alertou que a imagem tem 35.547 bytes e eu confirmei o uso da imagem.
6. O GPG pediu uma confirmação para garantir que a imagem era a que eu queria anexar, e eu confirmei.
7. A imagem foi atrelada à chave com sucesso.

```
sec  ed25519/F494AF6DB734A9CE
     criada: 2025-05-15  expira: 2028-05-15  uso: SC
     confiança: plena      validade: plena
ssb  cv25519/2A6272B06D7E3BE0
     criada: 2025-05-15  expira: 2028-05-15  uso: E
[  plena  ] (1). Jessica Regina dos Santos <jessicars241@gmail.com>
[desconhec.] (2) [jpeg image of size 35547]
```

8. Imagem associada à chave (KEY ID: F494AF6DB734A9CE):



Questão 9) O que é preciso para criar e manter um servidor de chaves PGP sincronizado com os demais servidores existentes?

Primeiramente, o servidor deve utilizar um software compatível com o protocolo OpenPGP. Um requisito fundamental para sincronização entre servidores é o suporte a protocolos que permitam a replicação automática de chaves entre eles. Em modelos recentes, a sincronização pode ocorrer via APIs centralizadas que implementam mecanismos de verificação de identidade e políticas de privacidade (OpenPGP.org, 2023)

Do ponto de vista operacional, a manutenção de um servidor de chaves necessita de uma infraestrutura robusta, com conexão estável e armazenamento seguro para o banco de dados de chaves. Além disso, é necessário implementar políticas de segurança para evitar abusos (Koch et al., 2023).

A conformidade com a lei também é importante, especialmente no tratamento de dados pessoais. Aderir a legislações locais, como a LGPD no Brasil, garante que os dados armazenados sejam tratados com responsabilidade (Koch et al., 2023).

Questão 10)

Para testar o sigilo de arquivos com criptografia PGP, também foi utilizado o software Kleopatra. Inicialmente, eu e minha dupla trocamos nossas chaves públicas. Em seguida, via Kleopatra, importei a chave pública da minha colega.

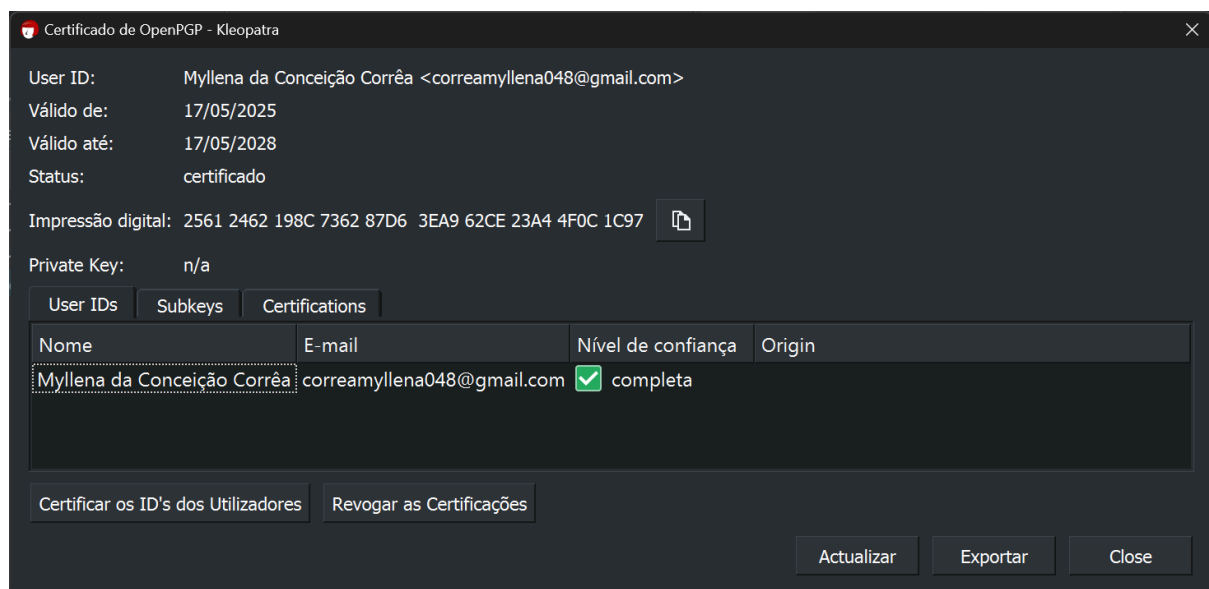
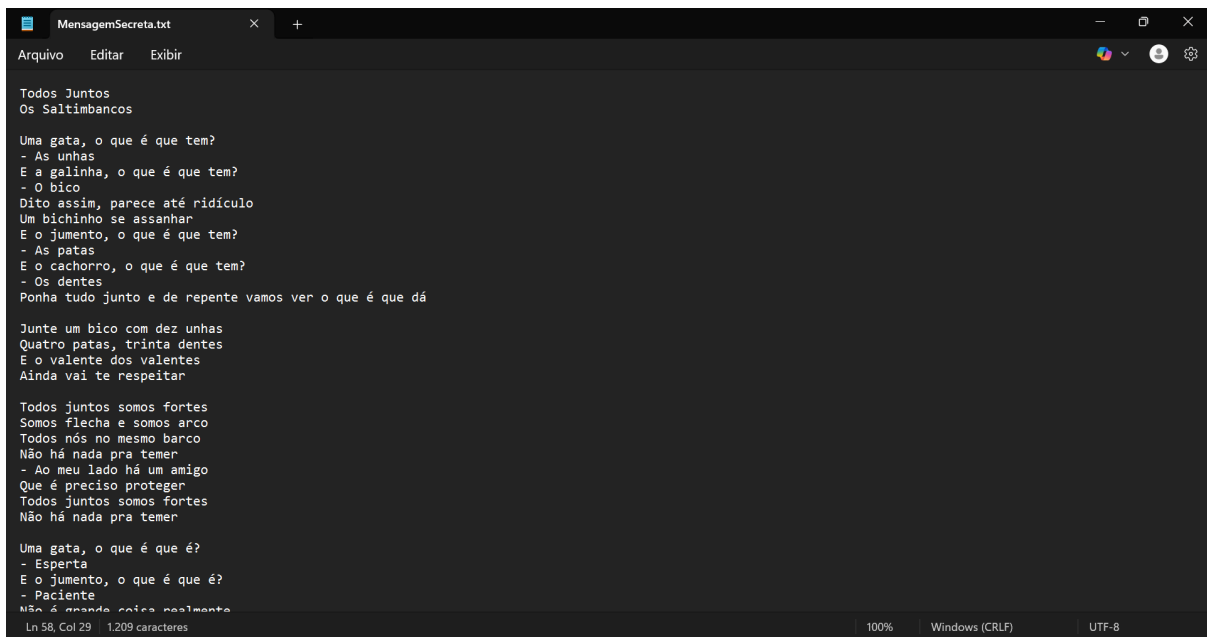


Imagem 6. Dados da chave pública da minha colega no Kleopatra.

Em seguida, foi cifrado o arquivo MensagemSecreta.txt (previamente criado com uma mensagem super secreta!), selecionando a chave pública da minha colega como destinatária. Foi gerado então o arquivo MensagemSecreta.txt.gpg, o qual foi enviado via fórum da disciplina.

Agora, apenas a Myllena, de posse da chave privada correspondente, conseguirá decifrar o conteúdo, garantindo o sigilo conforme os princípios de criptografia de chave pública (Koch et al., 2023). Esse processo evidencia o funcionamento prático da criptografia assimétrica a qual aprendemos em sala, onde a cifragem é feita com a chave pública e a decifragem com a chave privada do destinatário.



```
Arquivo  Editar  Exibir

Todos Juntos
Os Saltimbancos

Uma gata, o que é que tem?
- As unhas
E a galinha, o que é que tem?
- O bico
Dito assim, parece até ridículo
Um bichinho se assanhar
E o jumento, o que é que tem?
- As patas
E o cachorro, o que é que tem?
- Os dentes
Ponha tudo junto e de repente vamos ver o que é que dá

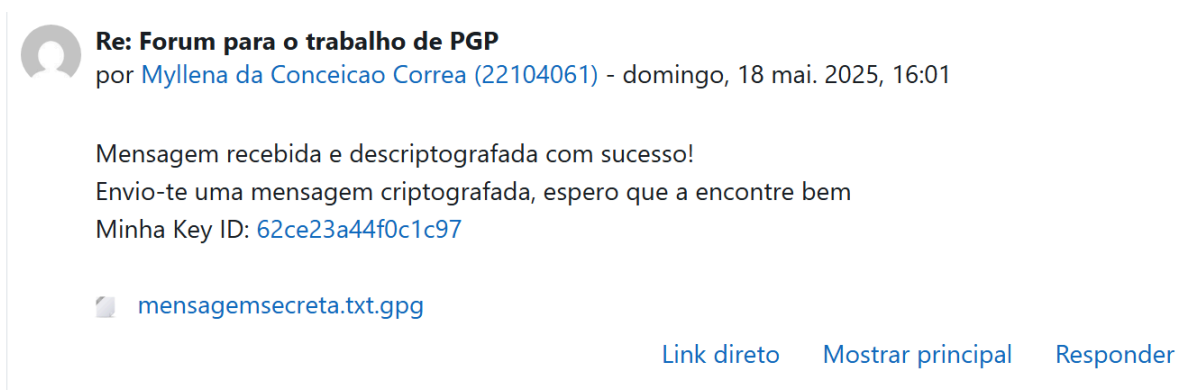
Junte um bico com dez unhas
Quatro patas, trinta dentes
E o valente dos valentes
Ainda vai te respeitar

Todos juntos somos fortes
Somos flecha e somos arco
Todos nós no mesmo barco
Não há nada pra temer
- Ao meu lado há um amigo
Que é preciso proteger
Todos juntos somos fortes
Não há nada pra temer

Uma gata, o que é que é?
- Esperta
E o jumento, o que é que é?
- Paciente
Não é grande coisa realmente


Ln 58, Col 29 | 1209 caracteres  100%  Windows (CRLF)  UTF-8
```

Imagem 6. A mensagem secreta enviada trata-se de uma letra de música.



Re: Forum para o trabalho de PGP
por [Myllena da Conceicao Correa \(22104061\)](#) - domingo, 18 mai. 2025, 16:01

Mensagem recebida e descriptografada com sucesso!
Envio-te uma mensagem criptografada, espero que a encontre bem
Minha Key ID: [62ce23a44f0c1c97](#)

 [mensagemsecreta.txt.gpg](#)

[Link direto](#) [Mostrar principal](#) [Responder](#)

Imagem 7. Confirmação Myllena e mensagem secreta (a ser descriptografada)

Após o envio do arquivo criptografado para minha colega, foi realizada a segunda etapa da atividade: o recebimento de um arquivo sigiloso e o processo de sua decriptação. Para isso, foi necessário ter minha chave privada previamente instalada no sistema, visto que a criptografia do arquivo recebido foi realizada utilizando minha chave pública (KEY ID: F494 AF6D B734 A9CE).

Ao receber o arquivo `mensagemsecreta.txt.gpg`, correspondente ao conteúdo criptografado, acessei o Kleopatra e utilizei a função Decriptografar/Verificar, disponível no menu principal. Após selecionar o arquivo recebido, o software iniciou o processo de decriptação automaticamente, solicitando a senha associada à minha chave privada para garantir a segurança da operação. Após a autenticação bem-sucedida, o Kleopatra conseguiu acessar o conteúdo criptografado e recuperar o arquivo original — no caso, um documento contendo a mensagem enviada pela Myllena (Imagem 8).

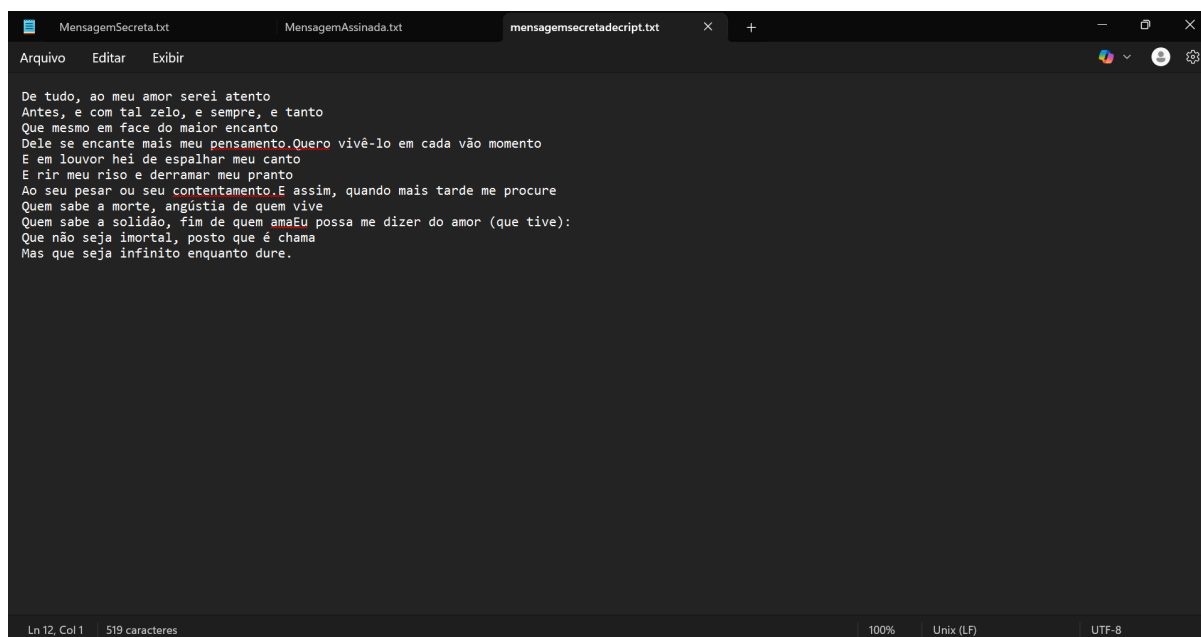


Imagem 8. Mensagem descriptografada com sucesso!

Esse procedimento demonstrou na prática o funcionamento do modelo de criptografia assimétrica que aprendemos em sala. Apenas o destinatário, possuidor da chave privada correta, é capaz de acessar o conteúdo criptografado pelo remetente com a chave pública correspondente.

Questão 11)

A assinatura digital é um dos principais recursos da criptografia de chave pública, pois nos garante a integridade e a autenticidade de arquivos, como aprendemos em sala. Segundo a *Free Software Foundation* (2023), a assinatura digital com PGP permite que o destinatário verifique se o conteúdo foi realmente enviado por quem diz ser o remetente e se ele não foi alterado no caminho.

Para esta questão, foram realizados testes práticos com dois tipos de assinaturas: assinatura anexada e assinatura separada.

1. Assinatura Digital Anexada

A assinatura foi embutida diretamente no conteúdo do arquivo original. Esse processo é conhecido como assinatura inline ou anexada ou *clear-signing*, onde o conteúdo assinado permanece legível em texto claro, juntamente com a assinatura digital (KOCH et al., 2023).

Infelizmente, o Kleopatra não possui suporte direto à assinatura anexada de mensagens. Para essa questão, realizei um procedimento alternativo (GnuPG em linha de comando):

1. Criei um arquivo MensagemAssinada.txt com seu conteúdo.

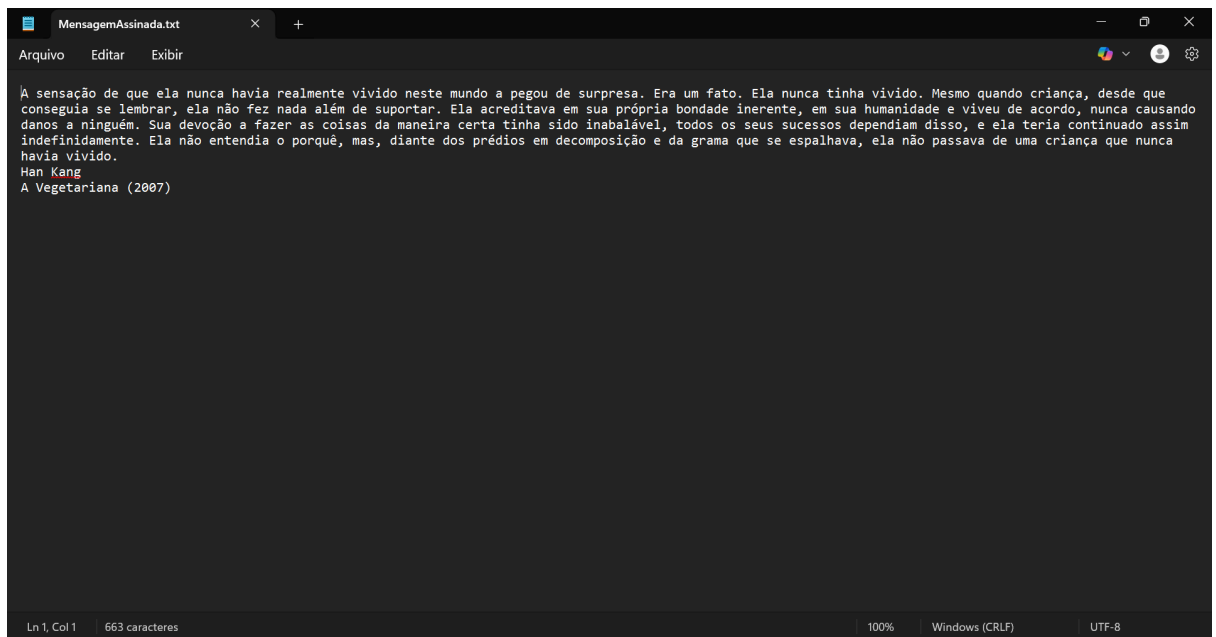
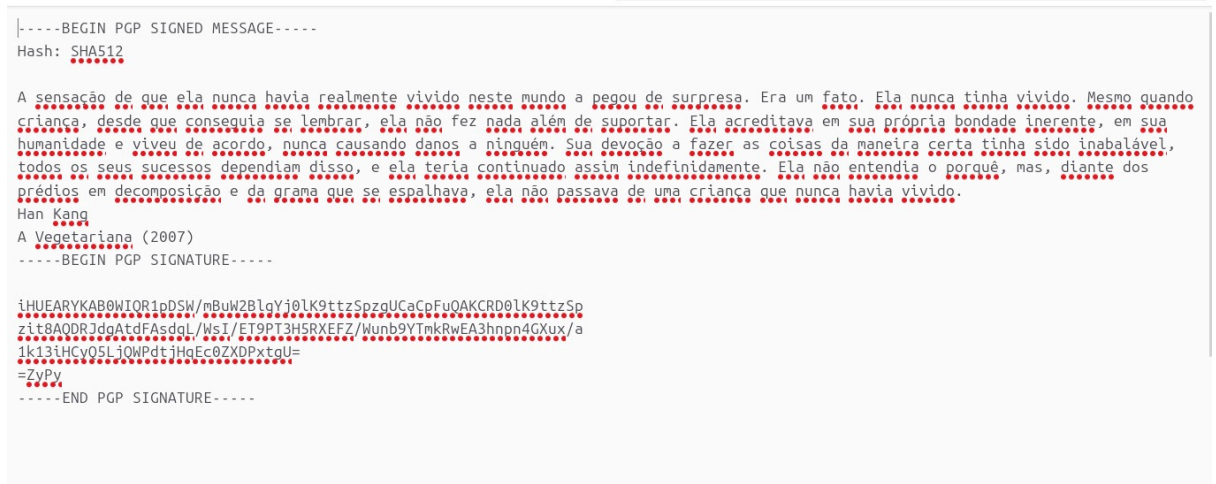


Imagem 9. Conteúdo de MensagemAssinada.txt

2. Abri o Prompt de Comando (cmd) do Windows.
3. Usei o comando: `gpg --clearsign MensagemAssinada.txt`
4. Isso gerou o arquivo `MensagemAssinada.txt.asc` com assinatura embutida (texto + assinatura).



2. Assinatura Digital Separada

Em seguida, realizou-se o processo de assinatura separada via Kleopatra.

O procedimento foi realizado com os seguintes passos:

1. Acessei o menu “Assinar/Criptografar” no Kleopatra.
2. Selecionei o arquivo desejado (MensagemAssinada.txt).

3. Foi marcada apenas a opção "Assinar".

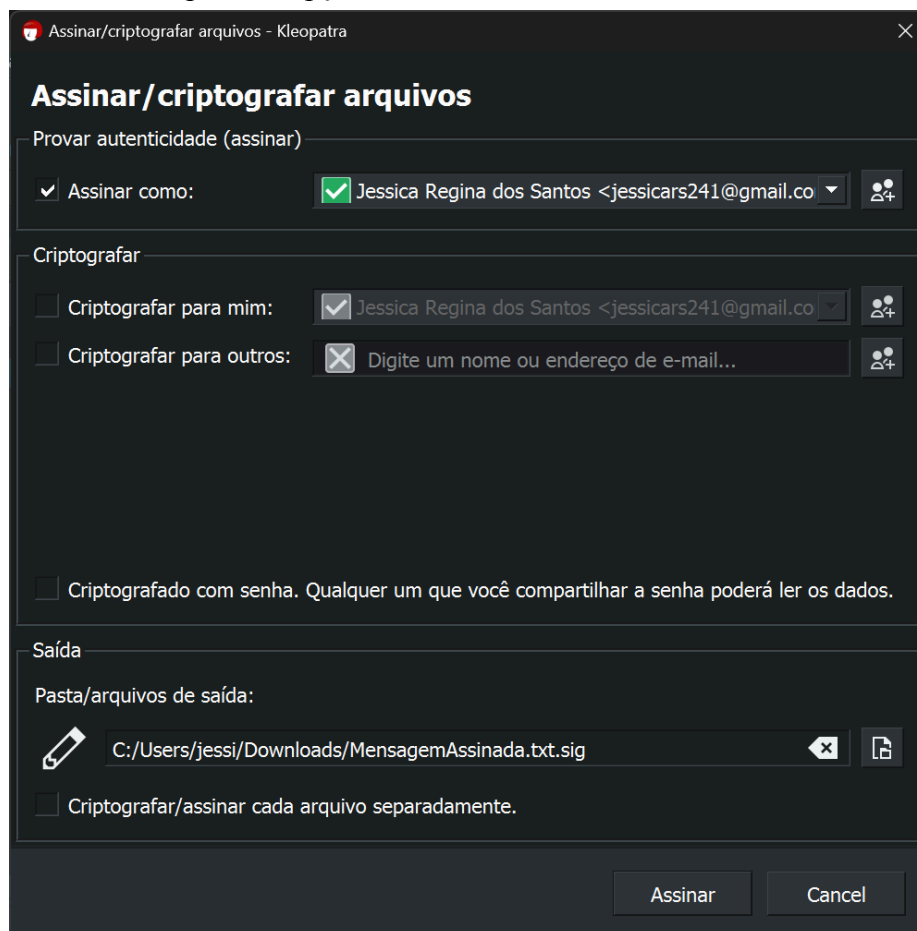


Imagem 10. Página no Kleopatra

4. O Kleopatra gerou automaticamente o arquivo MensagemAssinada.txt.sig, contendo um arquivo de assinatura.sig distinto do conteúdo original, que permaneceu intacto.



Re: Forum para o trabalho de PGP

por [Myllena da Conceicao Correa \(22104061\)](#) - domingo, 18 mai. 2025, 18:43

Assinaturas verificadas!!!

Segue as minhas para a sua verificação

[mensagemAssinada.txt](#)
 [mensagemAssinada.txt.asc](#)
 [mensagemAssinada.txt.sig](#)

[Link direto](#) [Mostrar principal](#) [Responder](#)

Imagem 11. Minha colega confirmou minhas assinaturas e enviou assinaturas para eu verificar.

Verificando a chave da minha colega, Myllena:

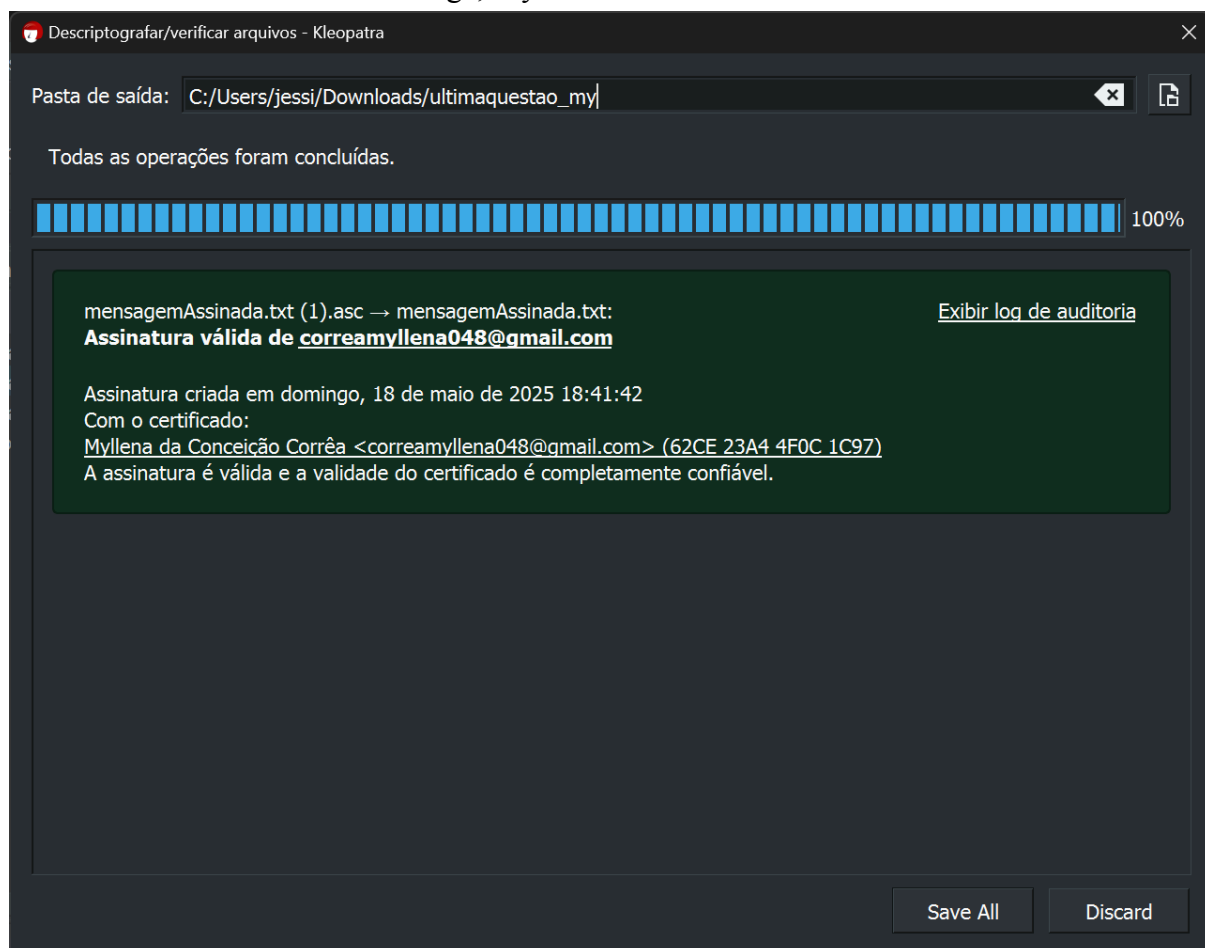


Imagem 12. Assinatura anexada da Myllena verificada com sucesso.

Referências

CALLAS, J. et al. *OpenPGP Message Format*. RFC 4880, IETF, 2007. Disponível em: <https://datatracker.ietf.org/doc/html/rfc4880>

GnuPG. *The GNU Privacy Guard Manual*, 2023. Disponível em: <https://gnupg.org/documentation/manuals/gnupg/>

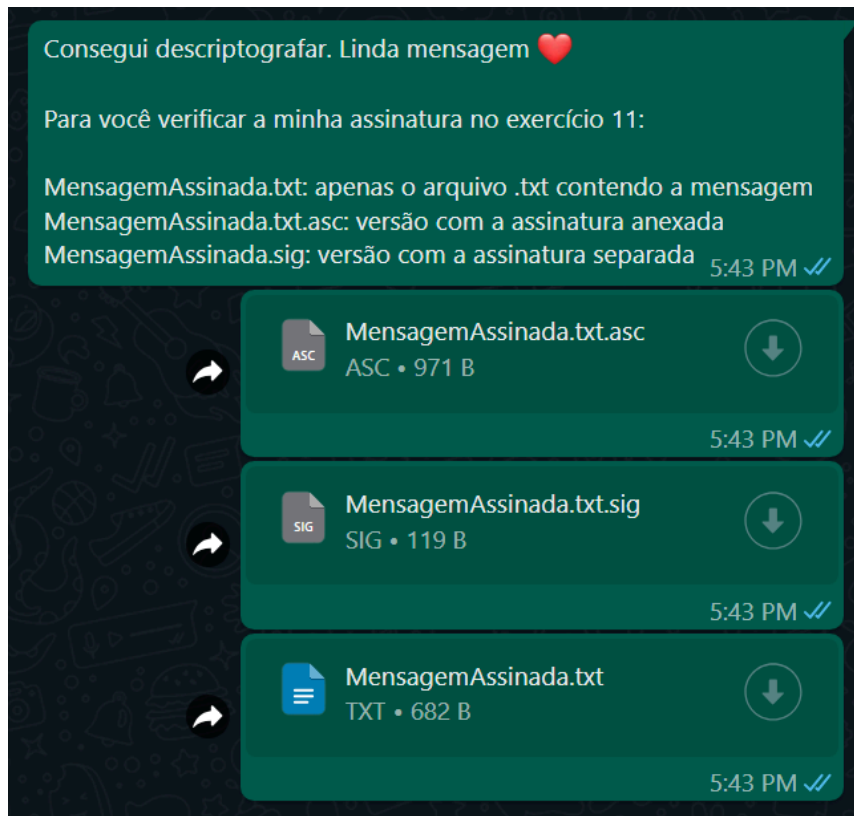
Gpg4win. *Documentation for Kleopatra and Gpg4win*, 2023. Disponível em: <https://gpg4win.org/doc/en/>

KOCH, Werner et al. *The GNU Privacy Handbook*. Free Software Foundation, 2023. Disponível em: <https://gnupg.org/documentation/>

OpenPGP.org. *OpenPGP Keyserver Protocols and Security Considerations*. 2023. Disponível em: <https://keys.openpgp.org/about>

Zimmermann, P. R. (1995). *The Official PGP User's Guide*. MIT Press.

Anexos



Errata da mensagem similar enviada no fórum.

Nova mensagem enviada a minha colega, em privado (não havia como editar ou excluir a mensagem errada no fórum).