UNIVERSIDADE FEDERAL DO CEARÁ

Departamento de Engenharia

Faculdade de Engenharia de Software

EQUIPE 4

José Vinícius Evangelista Dias de Souza – 537071

Erick Gabriel Ferreira Gaspar - 536261

João Pedro Pereira Holanda – 539012

Vitor Loula Silva - 540622

Francisco Paulino Arruda Filho - 528451

Pedro Henrique Santos Moreira - 536925

Ítalo Kauã Vitor Fernandes - 537595

TRABALHO 2 PGP

Professor: Michel Sales Bonfim

“Tudo que o homem ignora não existe para ele. Por isso, o universo de cada um se resume ao seu saber.”

~Albert Einstein.

1. CHAVE PÚBLICA: link

```
➜  ~ gpg --export -a "joseedsouza@alu.ufc.br" > chave_publica.asc
➜  ~ cat chave_publica.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEaSXuDRYJKwYBBAHaRw8BAQdAR9lAcqkM+Uno2OKn6uTSsic0t9RAcPQIvF7D
gabRKSO0Kkpvc8OpIFNvdXphICh6w6kpIDxqb3NlZWRzb3V6YUBhbHUudWZjLmJy
PoiZBBMWCgBBFiEE3IeEO9FPT1JvIa5GbWazM0MmdnoFAmkl7g0CGwMFCQB2pwAF
CwkIBwICIgIGFQoJCAsCBBYCAwECHgcCF4AACgkQbWazM0MmdnqRlgD/fLEJPIH0
qtKCj/6NxcJRH++VjbYx10Q2HmGNuRlRrtIBANnypTIJznUn7hNa8BQzl5jXAyO3
BKCOEKff9Lg7zoELuDgEaSXuDRIKKwYBBAGXVQEFAQEHQDA/twLa3oM1dQdnDom7
2Bt76KCwugRwzw0H/Q/bB0xGAwEIB4h+BBgWCgAmFiEE3IeEO9FPT1JvIa5GbWaz
M0MmdnoFAmkl7g0CGwwFCQB2pwAACgkQbWazM0Mmdnq5NQD9GLwXzETr8tMJ8PYO
ElyRYMrWvTI7UpAE4/FRiWOFuiUBAPUDfd24YdYfZr/pWNiagcxHuZCgnBkRZ6Rl
Pco8jH4H
=C5pH
-----END PGP PUBLIC KEY BLOCK-----
➜  ~ gpg --decrypt ./Downloads/palavra_equipe4.txt.asc
gpg: cifrado com chave cv25519, ID EF8B86540165D89D, criado em 2025-11-25
      "José Souza (zé) <joseedsouza@alu.ufc.br>"
equipe 4
```

2. Decifrar primeira mensagem:

```
➜  ~ gpg --decrypt ./Downloads/equipe3-msg_to_equipe4.txt.asc
gpg: cifrado com chave cv25519, ID EF8B86540165D89D, criado em 2025-11-25
      "José Souza (zé) <joseedsouza@alu.ufc.br>"
E ai os caras,
somos a equipe 3 show papito
➜  ~
```

3. Decifrar mensagens recebidas:

```
➜  ~ gpg --decrypt ./Downloads/palavra_grupo5_para_grupo4.asc
gpg: cifrado com chave cv25519, ID EF8B86540165D89D, criado em 2025-11-25
      "José Souza (zé) <joseedsouza@alu.ufc.br>"
equipe 5
```

4. Criptografia das mensagens enviadas:

```
➜  ~ gpg --import ./Downloads/equipe5.asc
gpg: chave B14DB36B9C1045F5: chave pública "equipe5 (sim) <thamires.taboza@gmail.com>" importada
gpg: Número total processado: 1
gpg:               importados: 1
➜  ~ echo "equipe 4" >> "equipe_4_para_equipe_5.txt"
➜  ~ gpg --encrypt --armor -r B2DB667B5C13D3DD379B66F0B14DB36B9C1045F5 equipe_4_para_equipe_5.txt
gpg: A75D76F428DE0B7C: Não há nenhuma garantia que esta chave pertence ao usuário nomeado

sub  cv25519/A75D76F428DE0B7C 2025-11-25 equipe5 (sim) <thamires.taboza@gmail.com>
 Impressão digital da chave primária: B2DB 667B 5C13 D3DD 379B  66F0 B14D B36B 9C10 45F5
      Impressão digital da sub-chave: C1EE 3592 CAAE A8C5 17CD  4D25 A75D 76F4 28DE 0B7C

Não se tem certeza de que esta chave pertence a pessoa listada
no identificador de usuário. Se você *realmente* sabe o que está
fazendo, pode responder sim à próxima pergunta

Usar esta chave de qualquer maneira? (y/N) y
➜  ~ cat equipe_4_para_equipe_5.txt
equipe 4
➜  ~ cat equipe_4_para_equipe_5.txt.asc
-----BEGIN PGP MESSAGE-----

hF4Dp1129CjeC3wSAQdA/fxSQ2kvWha4KTc0keOey2f6YAJZAfuvg/iJ38VBtQow
U1awqYVbnAhNgw5FA+Wndx4ht5qhfx805yn3IOCaBNNDGM3zmyszMO4TJhOcajoj
1F8BCQIQ7SHqgVyeI2PnWZ1QSWueWcAo7G5dcWcRV+OgGN7pXYVbB6gxvgoHn1AF
eAWjAuztOvxEZcSMGljZuskmKW3ySEqbD3Vu5ol/m08DU4LhkqR5vxuehq3hb1f6
nQ==
=iSFy
-----END PGP MESSAGE-----
```

```
➜  ~ echo "equipe 4" >> "equipe_4_para_equipe_3.txt"
➜  ~ gpg --import ./Downloads/chave_publica_equipe3.asc
gpg: chave A81067551C45DE28: chave pública "chave-equipe3 (show papito) <erickdev1218@alu.ufc.br>" importada
gpg: Número total processado: 1
gpg:               importados: 1
➜  ~ gpg --encrypt --armor -r 1950FE504E0A2B1AAADD29DFA81067551C45DE28 ./equipe_4_para_equipe_3.txt
gpg: AD2E349A84B50517: Não há nenhuma garantia que esta chave pertence ao usuário nomeado

sub  cv25519/AD2E349A84B50517 2025-11-25 chave-equipe3 (show papito) <erickdev1218@alu.ufc.br>
 Impressão digital da chave primária: 1950 FE50 4E0A 2B1A AADD  29DF A810 6755 1C45 DE28
      Impressão digital da sub-chave: 738A 226B 137D B1DE 719C  A17E AD2E 349A 84B5 0517

Não se tem certeza de que esta chave pertence a pessoa listada
no identificador de usuário. Se você *realmente* sabe o que está
fazendo, pode responder sim à próxima pergunta

Usar esta chave de qualquer maneira? (y/N) y
➜  ~ cat equipe_4_para_equipe_3.txt
equipe 4
➜  ~ cat equipe_4_para_equipe_3.txt.asc
-----BEGIN PGP MESSAGE-----

hF4DrS40moS1BRcSAQdAcvC6hjiiYBINKebgM3SAifEQjtdz3kY9Pl6jkLPPfUkw
lhH+FUQCRVvWcQvE9gqPkLNi7J5NwNq4ug/LzalbOxV5F8J1TnuE+AEeW4BEOqBN
1F4BCQIQe21U+x8nMtzywhwxG4VB9ZO2QnJPH8/Tz4JfiB/AUUpxjvSDQgcDuxaG
pLdgrCwF50NINqlXqE2tO2O+3GGxlRZ1/a+b80nvp9sPF7qy+whgKKOjCndS1APV
=Yiaz
-----END PGP MESSAGE-----
```

5.1. Qual a importância da criptografia de chave pública?

A criptografia de chave pública é relevante por que permite a comunicação segura entre duas partes mesmo em um meio não seguro, já que as duas partes só precisam compartilhar suas chaves públicas para descriptografia

5.2. Por que apenas o grupo destinatário pode descriptografar?

Porque a mensagem é assinada com a chave privada do remetente e a autenticidade verificada com base na chave pública dele. Além disso, as duas partes usam um segredo de sessão encriptado com a chave pública do destinatário e só pode ser decriptado com a chave privada dele. O que possibilita compartilhar uma mesma chave secreta para ser usada na comunicação sem que um intermediário consiga decifrar.

5.3. O que aconteceria se a chave privada fosse divulgada?

Caso a chave privada fosse vazada, uma pessoa poderia se passar por outra e enviar mensagens criptografadas para todos os indivíduos que reconhecem a chave pública correspondente. Por isso é tão importante armazenar a chave privada com segurança e invalidá-la em caso de comprometimento

Fonte: How PGP works