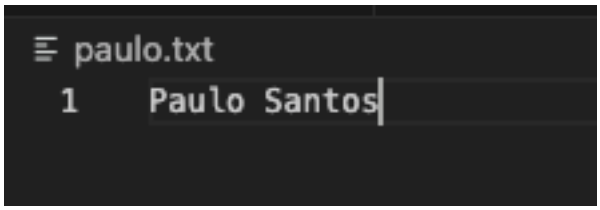
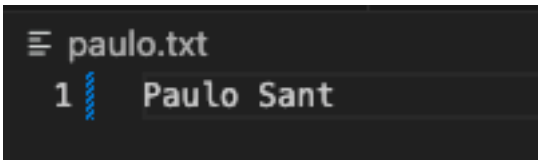
3. Criptografia com OpenSSL

A)

```
cotonet@Paulos-Mac-mini lab2-alunos % openssl dgst -sha512 paulo.txt
SHA2-512(paulo.txt)= 23776d0adbc24879e8255ccdbd37476be07c42c8e6fcf2f28175dd9a93730aa05a12fd269591bdaae930995a7365447d5ccba2a37746ea2f86593b91eb49751e
cotonet@Paulos-Mac-mini lab2-alunos % openssl dgst -sha512 paulo.txt
SHA2-512(paulo.txt)= 5f1e2e8197054b0a8a482d2ce35526cefd19874a436676b4b269bcd89bdc76fd20b325fa161e9ee275c53ac38ccc2664b38a509cd81845cd3dacfa4115bf0e35
cotonet@Paulos-Mac-mini lab2-alunos % openssl dgst -sha512 paulo.txt
SHA2-512(paulo.txt)= 23776d0adbc24879e8255ccdbd37476be07c42c8e6fcf2f28175dd9a93730aa05a12fd269591bdaae930995a7365447d5ccba2a37746ea2f86593b91eb49751e
cotonet@Paulos-Mac-mini lab2-alunos %
```





B)

```
cotonet@Paulos-Mac-mini Princípios Técnicos em Cibersegurança % openssl dgst -sha512 -hmac "cncs--2025" Lab2-enunciado.pdf
HMAC-SHA2-512(Lab2-enunciado.pdf)= ac8d8bc1ddb8cf5baad528e5193845542b39a01fb7cec594fd00b32b1b5025dc5cb620fbf3648b23cb5c288aab8736e98051070aa435d96d08198ef648bb66a5
```

Chave: cncs--2025

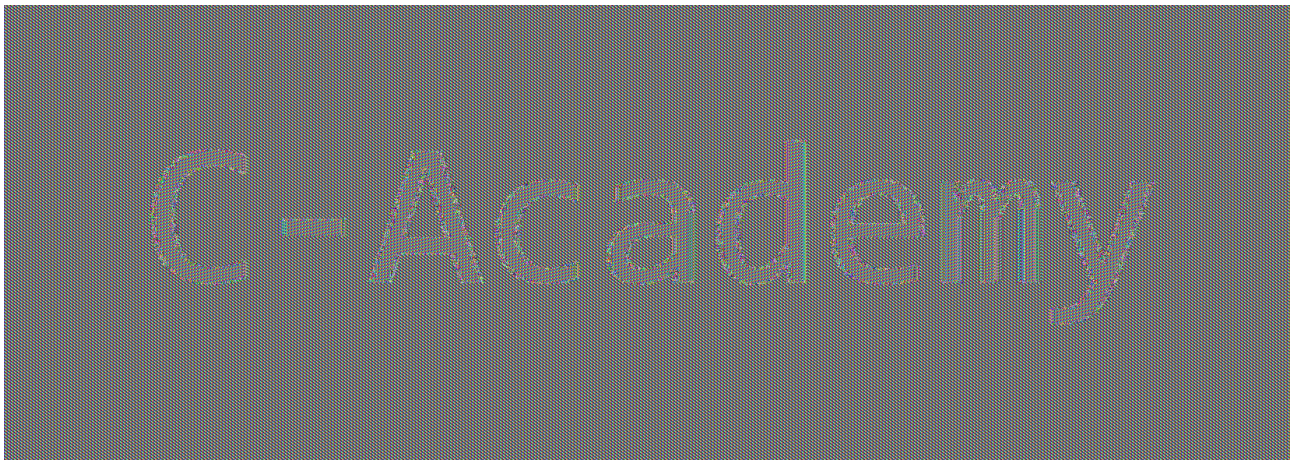
C)

Chave: cncs--2025

D)

CBC

EBC



E)

x_dec.pdf

	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded Text
00000000	25 50 44 46 2D 31 2E 35 0D 0A 25 B5 B5 B5 B5 0D	%PDF-1.5..%.....
00000010	0A 31 20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70	.1 0 obj..<</Typ
00000020	65 2F 43 61 74 61 6C 6F 67 2F 50 61 67 65 73 20	e/Catalog/Pages
00000030	32 20 30 20 52 2F 4C 61 6E 67 28 70 74 2D 50 54	2 0 R/Lang(pt-PT
00000040	29 20 2F 53 74 72 75 63 74 54 72 65 65 52 6F 6F	) /StructTreeRoo
00000050	74 20 36 38 20 30 20 52 2F 4D 61 72 6B 49 6E 66	t 68 0 R/MarkInf
00000060	6F 3C 3C 2F 4D 61 72 6B 65 64 20 74 72 75 65 3E	o<</Marked true>
00000070	3E 3E 3E 0D 0A 65 6E 64 6F 62 6A 0D 0A 32 20 30	>>>..endobj..2 0
00000080	20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70 65 2F 50 61	obj..<</Type/Pa
00000090	67 65 73 2F 43 6F 75 6E 74 20 38 2F 4B 69 64 73	ges/Count 8/Kids
000000A0	5B 20 33 20 30 20 52 20 31 32 20 30 20 52 20 32	[3 0 R 12 0 R 2
000000B0	31 20 30 20 52 20 32 39 20 30 20 52 20 34 35 20	1 0 R 29 0 R 45
000000C0	30 20 52 20 35 39 20 30 20 52 20 36 32 20 30 20	0 R 59 0 R 62 0
000000D0	52 20 36 34 20 30 20 52 5D 20 3E 3E 0D 0A 65 6E	R 64 0 R] >>..en
000000E0	64 6F 62 6A 0D 0A 33 20 30 20 6F 62 6A 0D 0A 3C	dobj..3 0 obj..<
000000F0	3C 2F 54 79 70 65 2F 50 61 67 65 2F 50 61 72 65	</Type/Page/Pare
00000100	6E 74 20 32 20 30 20 52 2F 52 65 73 6F 75 72 63	nt 2 0 R/Resourc
00000110	65 73 3C 3C 2F 58 4F 62 6A 65 63 74 3C 3C 2F 49	es<</XObject<</I

Data Inspector

binary	00111100
octal	074
uint8	60
int8	60
uint16	12092
int16	12092
uint24	5517116
int24	5517116
uint32	2035560252
int32	2035560252
uint64	5777948380685938492
int64	5777948380685938492
ULEB128	60
SLEB128	60
float16	0.113037109375
bfloat16	1.709850039333105e-10
float32	6.885781005940662e+34

```
cotonet@Paulos-Mac-mini lab2-alunos % openssl dgst -sha256 -verify public-key.pem -signature signature.bin x_dec.pdf
Verified OK
cotonet@Paulos-Mac-mini lab2-alunos % openssl dgst -sha256 -verify public-key.pem -signature signature.bin x_dec.pdf
Verification failure
80A001EE01000000:error:02000068:rsa routines:ossl_rsa_verify:bad signature:crypto/rsa/rsa_sign.c:442:
80A001EE01000000:error:1C880004:Provider routines:rsa_verify_directly:RSA lib:providers/implementations/signature/rsa_sig.c:1042:
cotonet@Paulos-Mac-mini lab2-alunos % openssl dgst -sha256 -verify public-key.pem -signature signature.bin x_dec.pdf
Verified OK
cotonet@Paulos-Mac-mini lab2-alunos %
```

x_dec.pdf

	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded Text
00000000	25 50 44 46 2D 31 2E 35 0D 0A 25 B5 B5 B5 B5 0D	%PDF-1.5..%.....
00000010	0A 31 20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70	.1 0 obj..<</Typ
00000020	65 2F 43 61 74 61 6C 6F 67 2F 50 61 67 65 73 20	e/Catalog/Pages
00000030	32 20 30 20 52 2F 4C 61 6E 67 28 70 74 2D 50 54	2 0 R/Lang(pt-PT
00000040	29 20 2F 53 74 72 75 63 74 54 72 65 65 52 6F 6F	) /StructTreeRoo
00000050	74 20 36 38 20 30 20 52 2F 4D 61 72 6B 49 6E 66	t 68 0 R/MarkInf
00000060	6F 3C 3C 2F 4D 61 72 6B 65 64 20 74 72 75 65 3E	o<</Marked true>
00000070	3E 3E 3E 0D 0A 65 6E 64 6F 62 6A 0D 0A 32 20 30	>>>..endobj..2 0
00000080	20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70 65 2F 50 61	obj..<</Type/Pa
00000090	67 65 73 2F 43 6F 75 6E 74 20 38 2F 4B 69 64 73	ges/Count 8/Kids
000000A0	5B 20 33 20 30 20 52 20 31 32 20 30 20 52 20 32	[3 0 R 12 0 R 2
000000B0	31 20 30 20 52 20 32 39 20 30 20 52 20 34 35 20	1 0 R 29 0 R 45
000000C0	30 20 52 20 35 39 20 30 20 52 20 36 32 20 30 20	0 R 59 0 R 62 0
000000D0	52 20 36 34 20 30 20 52 5D 20 3E 3E 0D 0A 65 6E	R 64 0 R] >>..en
000000E0	64 6F 62 6A 0D 0A 33 20 30 20 6F 62 6A 0D 0A 3C	dobj..3 0 obj..<
000000F0	3C 3E 2F 54 79 70 65 2F 50 61 67 65 2F 50 61 72	<>/Type/Page/Par
00000100	65 6E 74 20 32 20 30 20 52 2F 52 65 73 6F 75 72	ent 2 0 R/Resour
00000110	63 65 73 3C 3C 2F 58 4F 62 6A 65 63 74 3C 3C 2F	ces<</XObject<</
00000120	49 6D 61 67 65 35 20 35 20 30 20 52 3E 3E 2F 45	Image5 5 0 R>>/E

Data Inspector

binary	00101111
octal	057
uint8	47
int8	47
uint16	21551
int16	21551
uint24	7951407
int24	7951407
uint32	1886999599
int32	1886999599
uint64	7012156732541064239
int64	7012156732541064239
ULEB128	47
SLEB128	47
float16	66.9375
bfloat16	3006477107200
float32	3.08654156662349e+29
float64	5.688715372919898e+160
GUID	End of File