Part1

**Citala espartana**

Calendar

Description automatically generated with low confidence

Vinaigrette

A picture containing text, newspaper

Description automatically generated

**Alberti cifer**

Text

Description automatically generated with low confidenceA picture containing chart

Description automatically generated

**Bellaso-Vigen`ere**

Key: “BELLASO”

A picture containing text, clock

Description automatically generated

Relação de congruencia

Se a ≡ a(modn) -> (reﬂexividade)

Se a ≡ b(modn) ent˜ao b ≡ amod(n) -> (simetria)

Se a ≡ b(modn) e b ≡ c(modn) então a ≡ c(modn) -> (transitividade)

(−a)(modn) = (n − a)(modn)

1(modn) = n + 1(modn)

0(modn) = n(modn) = 2n(modn)

Bitwise add, designado por n

bitwise XOR, designado por ⊕

bitwise OR, designado por ∨

bitwise AND, designado por ∧

complemento bitwise, designado por ¬

**cifra de hill**

A picture containing text, clock

Description automatically generated

modo ECB - Electronic CodeBook Mode;

modo CBC - Cipher Block Chaining Mode;

Text

Description automatically generated

modo OFB - Output Feedback Mode;

modo CFB - Cipher FeedBack Mode;

modo CTR - Counter Mode.

A picture containing text

Description automatically generated

**Padding**

OneAndZeros -> primeiro valor 1 (80 em hex) e resto é 0

Trailing Bit Complement -> complementa com o bit oposto

Text

Description automatically generated

aφ(n) ≡ 1(modn)



Se p, q são co-primos, φ(p · q) = (p − 1)(q − 1)

Se r ≡ s(modφ(n)) então ar ≡ as(modn)

r · t ≡ 1 modφ(n) então(xr)t ≡ x mod(n)

**Teorema RSA**

N=p\*q

A picture containing icon

Description automatically generated

Text

Description automatically generated

Encriptar -> rsa(x) = x^e \* mod(n)

Desencriptar -> rsa^−1(y) = y^d \* mod(n)

**O Protocolo Diﬃe-Hellman**

* 1 ≤ x ≤ p – 2
* 1 ≤ y ≤ p – 2
* A = αx (mod p) - Alice envia A para Bob
* B = αy (mod p) - Bob envia B para Alice
* Alice calcula K = Bx = (αy)x
* Bob calcula K = Ay = (αx)y.

Cifra ElGamal

Text

Description automatically generated

Text, letter

Description automatically generated

Text

Description automatically generated with medium confidence

**Merkle-Damgard**

sequências de s bits -> sequências de n bits, com s > n e deﬁne-se L = s − n.

1. OneZeroesPadding
2. Adicionar bloco de comprimento
3. 

**Curvas elípticas**



se A = (x A , y A ) então −A = (x A , −y A )

Text

Description automatically generated

Text

Description automatically generated

**ECC – Elliptic Curve Cryptography** Graphical user interface, text, application

Description automatically generated

**SHA-256**

mensagem M de comprimento arbitrário r

1. OneAndZeroes padding, de modo a obter um comprimento que seja múltiplo de 512 bits mas reservando os últimos 64 bits para a representação binária de r
2. A mensagem ´e subdividida em blocos m = m 1 ||m 2 || · · · ||m N cada um com comprimento 512-bits
3. Os blocos são processados sucessivamente, iniciando com um hash value H 0 ﬁxo e gerando os valores hash intermédios H i (com 256-bits) através de uma cifra por blocos C especifica do SHA-2:

**Davies-Meyer** :

HMAC

Text

Description automatically generated



Part2

**Conceitos base de segurança**

Confidencialidade

• Ausência de divulgação não autorizada de informação

• Garantida por meios criptográficos ou de controlo de acessos

Integridade

• Ausência de alterações não autorizadas ao sistema ou à informação

• Verificada por meios criptográficos ou de controlo de acessos

A política de segurança determina o que é autorizado ou não

Disponibilidade

• Prontidão do sistema para fornecer o serviço ou disponibilizar a informação

**Classificação**

• Projecto

• Vulnerabilidade durante a fase de definição de requisitos e desenho da arquitetura.

• Ex.: Não ter em conta todos os cenários onde a comunicação pode ser observada

• Codificação

• Erro de código (bug) com implicações de segurança

• Ex: validação insuficiente do input

• Operacional

• Vulnerabilidade causada por erro de configuração ou pelo ambiente de execução

• Ex.: contas sem palavras-passe