Esquema de Cifra Assimétrica

Algoritmos (G, E, D):

- G, função (probabilística) de geração de pares de chaves (KeyPairs)

$$KeyPairs \subseteq PublicKeys \times PrivateKeys$$

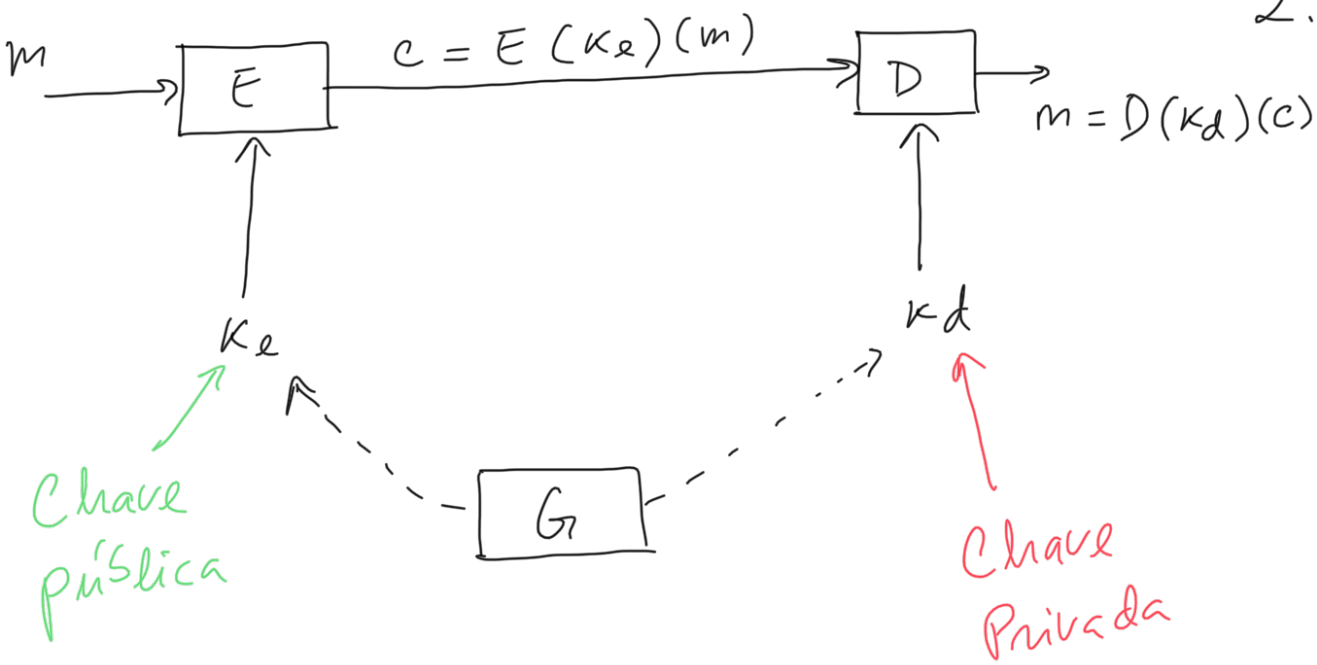
↑ Produto Cartesiano (conjunto dos pares ordenados (x, y) cujo $x \in PublicKeys$ e $y \in PrivateKeys$)

- E, função (probabilística) de cifra

$$E: PublicKeys \times PlainTexts \to CipherTexts$$

- D, função (determinística) de decifra

$$D: PrivateKeys \times CipherTexts \to PlainTexts$$



Propriedades:

Correção: $\forall m \in M, \forall (ke, kd) \in KeyPairs:$

$$D(kd)(E(ke)(m)) = m$$

Segurança: É computacionalmente infazível obter m a partir de c, sem conhecer kd.

- as mensagens ∈ PlainTexts são sequências de bits com dimensão menor do que o limite definido pelo esquema (ex: RSA 1024 bits)

$m < 1024$ bits

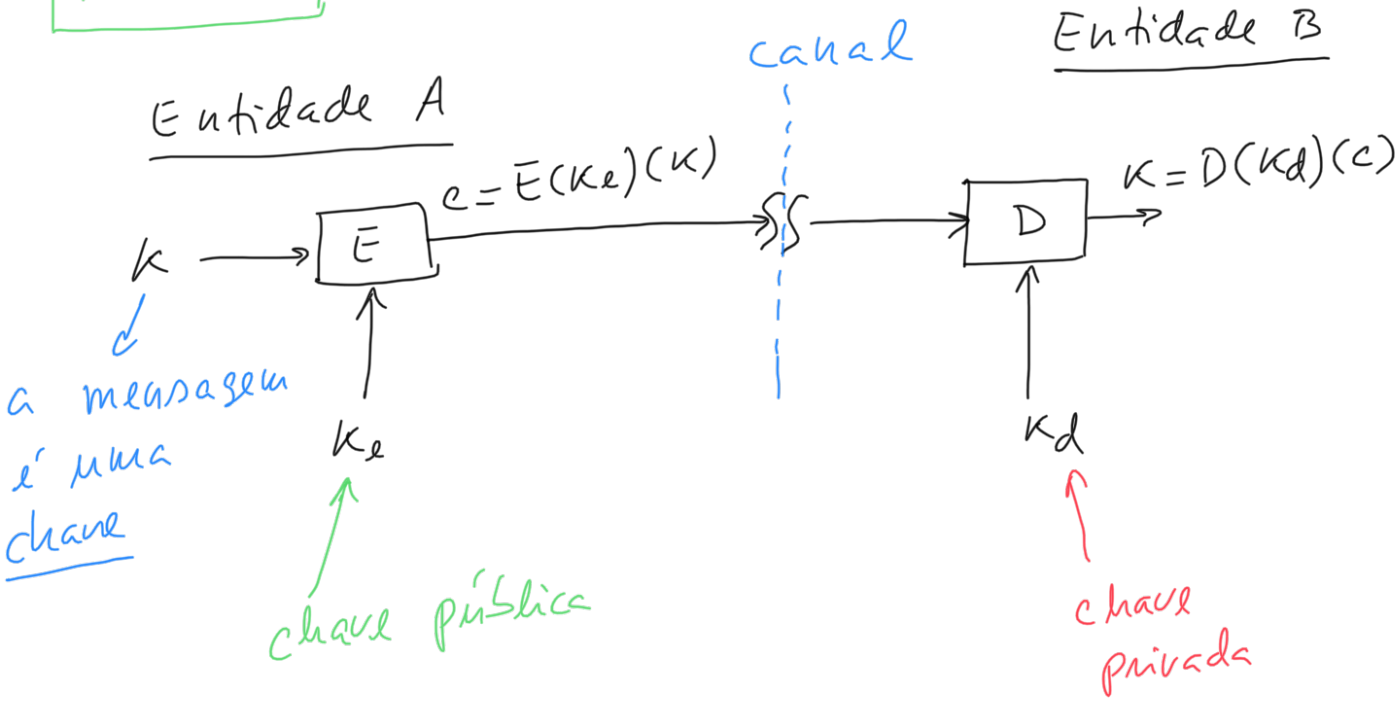
- Idem para os Criptogramas ∈ CiphrenTexts

- Cifra assimétrica não garante integridade

- A cifra assimétrica, devido ao elevado custo computacional e limitações na dimensão das sequências de bits, é usado num algoritmo híbrido.

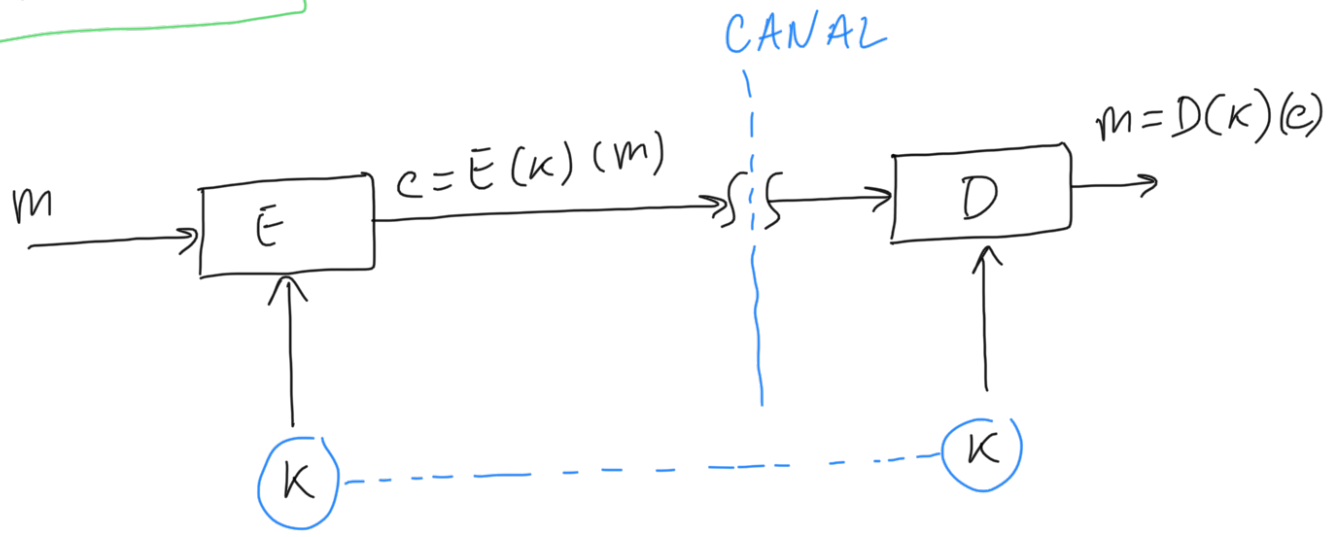
Algoritmo Híbrido

Passo 1



1. Estabelecimento de chave usando cifra assimétrica

Passo 2



2. Cifra simétrica usada para comunicação (por ser mais rápida)

Esquema de Assinatura Digital

Algoritmos (G, S, V):

- G, função (probabilística) de geração de pares de chaves (KeyPairs)

$$KeyPairs \subseteq PublicKeys \times PrivateKeys$$

- S, função (probabilística) de assinatura

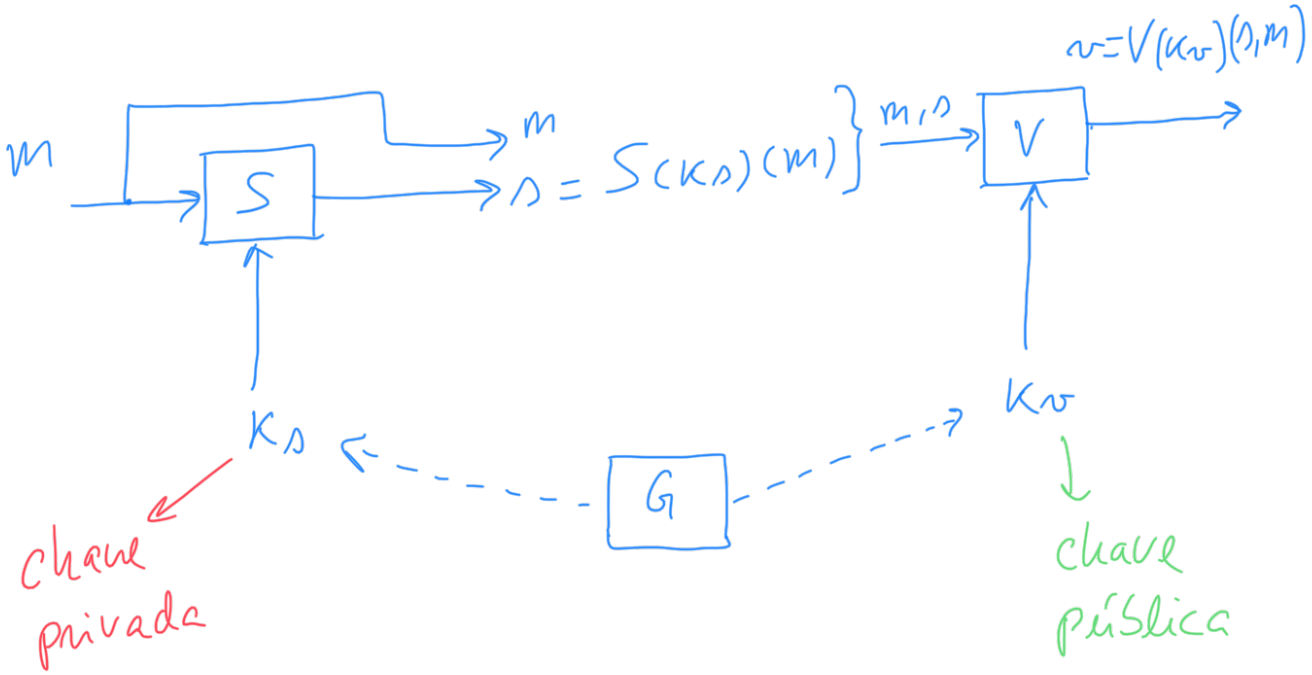
$$S : PrivateKeys \times \{0,1\}^* \longrightarrow Signatures$$

(m (mensagem))

- V, função (determinística) de verificação

$$V : PublicKeys \times (Signatures \times \{0,1\}^*) \rightarrow \{true, false\}$$

(m)



Propriedades:

Correção: $\forall m \in \{0,1\}^*$, $\forall (k_s, k_v) \in \text{keyPairs}$:

$$V(k_v)(S(k_s)(m), m) = \text{true}$$

Segurança:

Seja o conhecimento de k_s é computacionalmente infazível

- **falsificação seletiva** – dado m, encontrar s tal que $V(k_v)(s, m) = \text{true}$
- **falsificação existencial** – encontrar o par (m, s) tal que $V(k_v)(s, m) = \text{true}$

nota: k_v é conhecido

- Assinatura s tem tipicamente dimensão fixa, ex: 1024 bits
- Custo computacional maior do que os esquemas simétricos