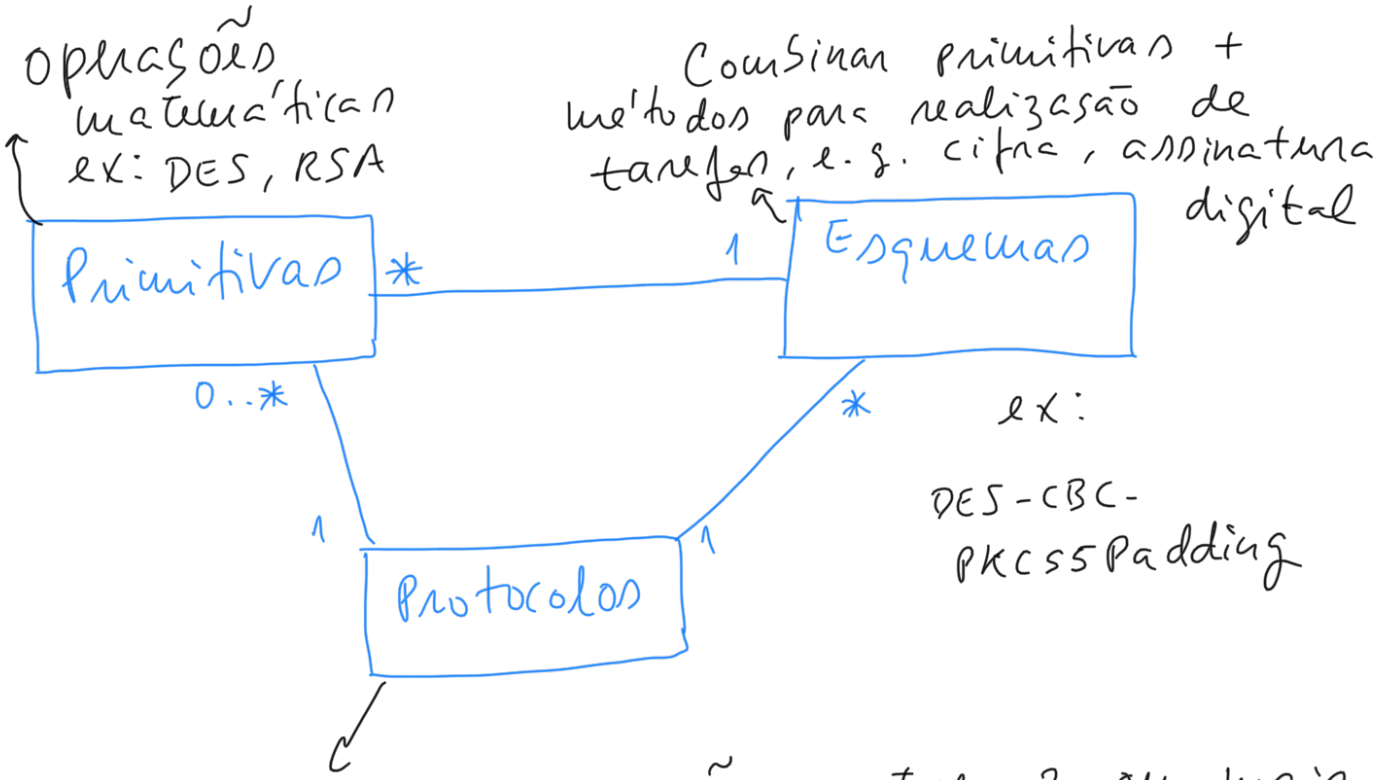
Mecanismos Criptográficos



Sequência de operações entre 2 ou mais entidades, com características seguras

ex: TLS_RSA_with_DES_CBC_SHA

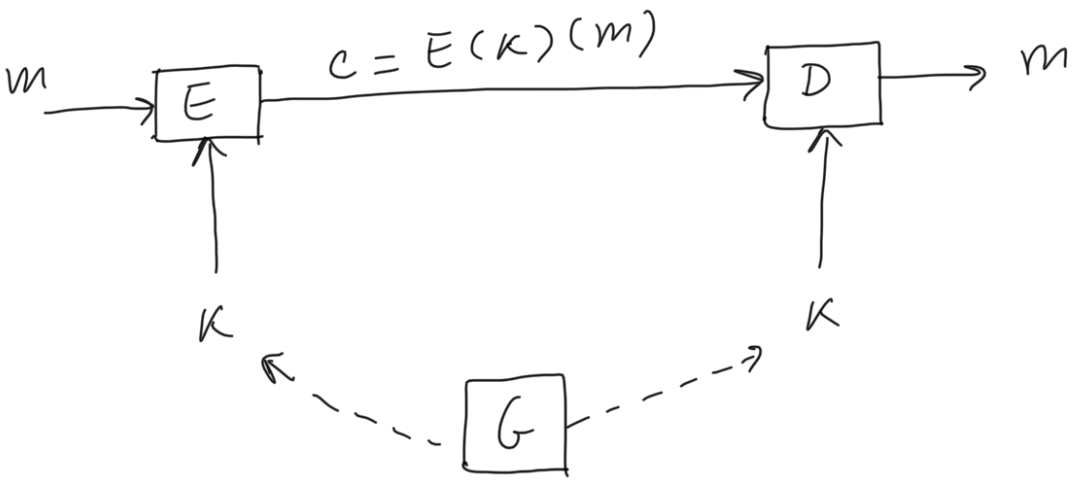
Um sistema criptográfico é um tuplo $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ onde:

- $\mathcal{P}$ é o conjunto dos textos em claro
- $\mathcal{C}$ é o conjunto dos criptogramas
- $\mathcal{K}$ é o conjunto das chaves
- $\mathcal{E} = \{ E(k) : k \in \mathcal{K} \}$ é o conjunto de funções de cifra $E(k) : \mathcal{P} \to \mathcal{C}$
- $\mathcal{D} = \{ D(k) : k \in \mathcal{K} \}$ é o conjunto de funções de decifra $D(k) : \mathcal{C} \to \mathcal{P}$

- Para todo o $e \in K$, existe um $d \in K$ tal que:

$$D(d)(E(e)(P)) = P,$$ para todos os textos em claro $P \in \mathcal{P}$

Num esquema simétrico, $d = e$.



G - Função probabilística de geração de chaves de dimensão n, i.e. $\{0,1\}^n$ (sequência de bits)

E - Função probabilística de cifra.

D - Função determinística de decifra.

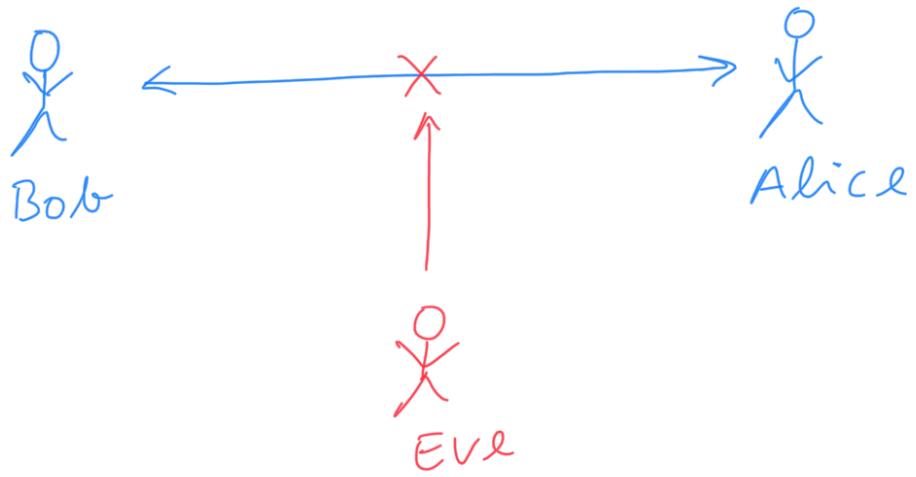
m e c são sequências arbitrárias de bits $\{0,1\}^*$

Propriedade de segurança:

É computacionalmente infazível obter m a partir de c, sem o conhecimento de k.

Ataque "Man-In-The-Middle" (MITM)

As comunicações pode estar sujeitas ao ataque MITM, onde o atacante intercepta mensagens da origem, altera-as, e reenvia para o destino.



VER EXEMPLO CÓDIGO PYTHON - MITM

O esquema de autenticação MAC (Message Authentication code) foi proposto para detetar alterações na mensagem e verificar a autenticidade do emissor.

Esquema de Autenticação - MAC (Message Authentication Code)

Algoritmos (G, T, V)

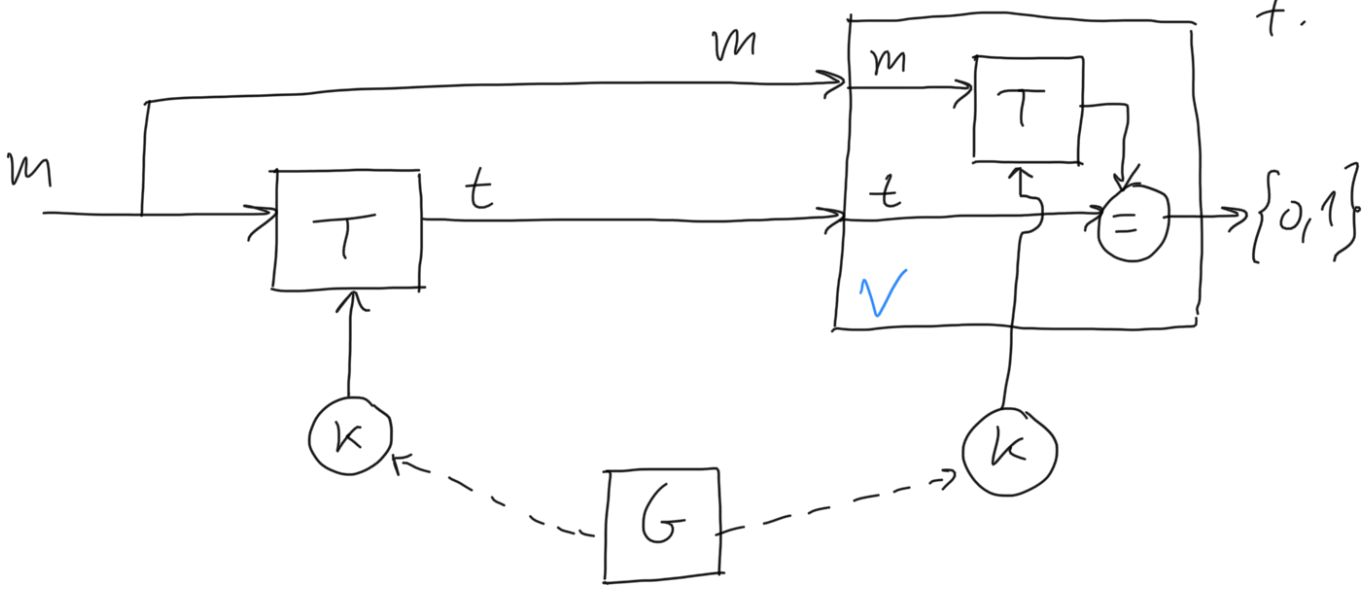
- G, função (probabilística) que gera chaves $k \in \mathcal{K}$
- T, função (probabilística[1]) que gera marcas (códigos) ("tag")
- V, função (determinística) que dados uma chave, uma mensagem e uma marca, retorna a validade da marca.

$$t = T(k)(m)$$

$$v = V(k)(t, m), \quad v \in \{0, 1\}$$

Nota:

[1] Pode ser determinístico também, e.g., no algoritmo HMAC.



Se T é determinístico então $V(k)(t, m)$:

$T(k)(m) = t$.

Propriedades:

Correção: $\forall\, m \in \{0,1\}^*, \forall\, k \in \mathcal{K}$:

$$V(k)(T(k)(m), m) = \text{true}$$

Segurança: Sem conhecer a chave k, é computacionalmente infazível fazer:

- falsificação seletiva (selective forgery)

O atacante é capaz de produzir um par (novo texto, MAC) para um texto à sua escolha (ou parcialmente controlado por ele/ela) tal que

$V(K)$ (MAC, novo texto) = true,

i.e., dado m, encontrar t tal que

$V(K)(t, m)$ = true.

- falsificação existencial (existential forgery)

O atacante é capaz de produzir um par (novo texto, MAC), mas sem controlo sobre o valor do novo texto, i.e., encontrar o par (m, t) tal que

$V(K)(t, m)$ = true.

Os ataques MAC permitem que um adversário consiga enviar um texto falsificado e que este seja aceite como autêntico.

- mensagem m é uma sequência de bytes de dimensão variável
- marca t (tag, MAC) tem tipicamente dimensão fixa (ex: 128, 160, 256 bits)