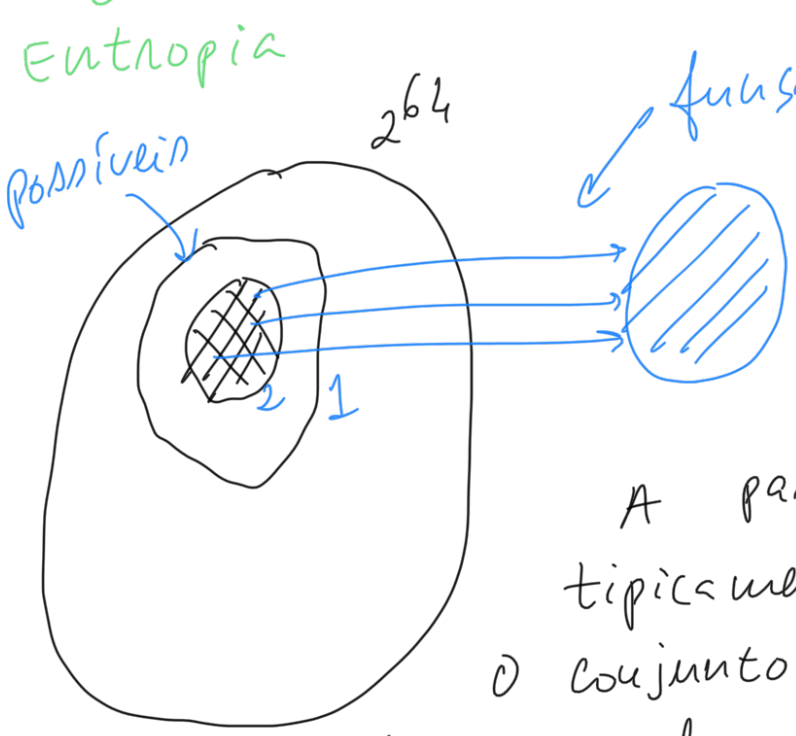
Derivação de chaves a partir de password – Password based encryption

password ⟶ { - chave, - IV }

↓ Entropia

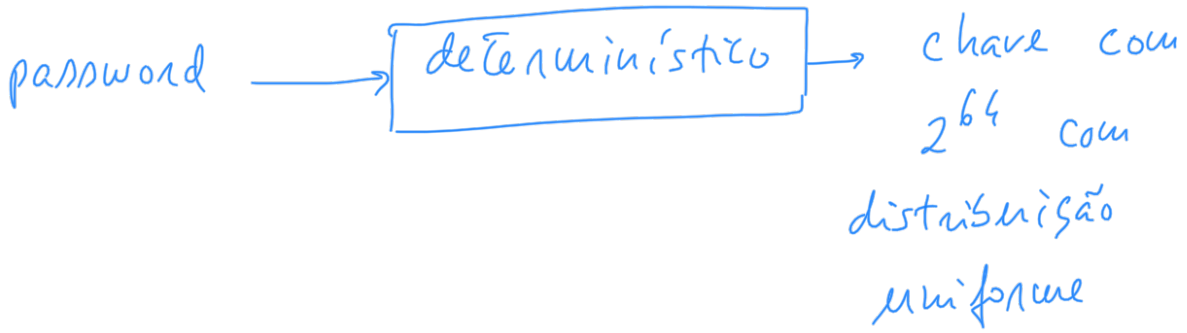


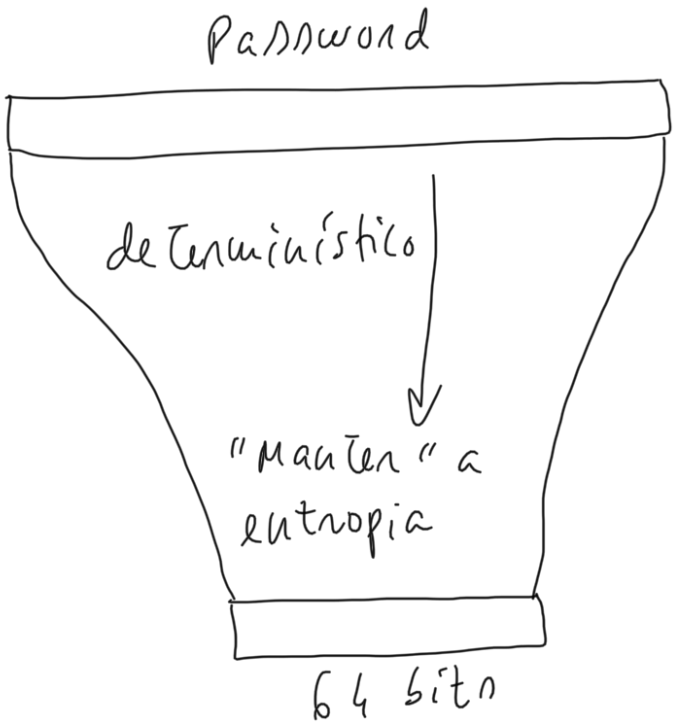
A password tem, tipicamente, pouca entropia.

O conjunto (1) é o conjunto de passwords possíveis (admitindo que só são usados caracteres printáveis).

O conjunto (2) é o conjunto de passwords mais prováveis.

Derivação de chaves a partir de password:





Entropia em Teoria de Informação

A entropia é o grau de casualidade, de indeterminação que algo possui.

A entropia está ligada à quantidade de informação:

- quanto maior a informação, maior a desordem, maior a entropia.
- quanto menor a informação, menor a escolha, menor a entropia.
- assim, a entropia quantifica a quantidade de incerteza envolvida no valor duma variável aleatória ou na saída dum processo aleatório.

Entropia:

$$H(X) = \sum p(x) \cdot \log_2 \left(\frac{1}{p(x)} \right)$$

Exemplo: Calcular entropia de lançar duas moedas ao ar

Evento de lançar 2 moedas e sair
Caras = 0
Coroas = 1

$p(a) = \frac{1}{2}$ → 00

$p(b) = \frac{1}{4}$ → 01

$p(c) = \frac{1}{4}$ → 10

$p(d) = 0$ → 11

$$H(X) = \frac{1}{2} \cdot 1 + \frac{1}{4} \cdot 2 + \frac{1}{4} \cdot 2 = 1{,}5 \text{ bit}$$

Convenção: $p(n) = 0$:

$0 \times \log 1/0 \equiv 0$ pois $\lim_{\theta \to 0^+} \theta \log 1/\theta = 0$.

→ Se moedas forem perfeitas (equiprováveis), $H(X) = 2$ bits

→ Se sair sempre caras (ou sempre coroas), $H(X) = 0$