# Cryptographie avancée

Anne Garcia-Sanchez

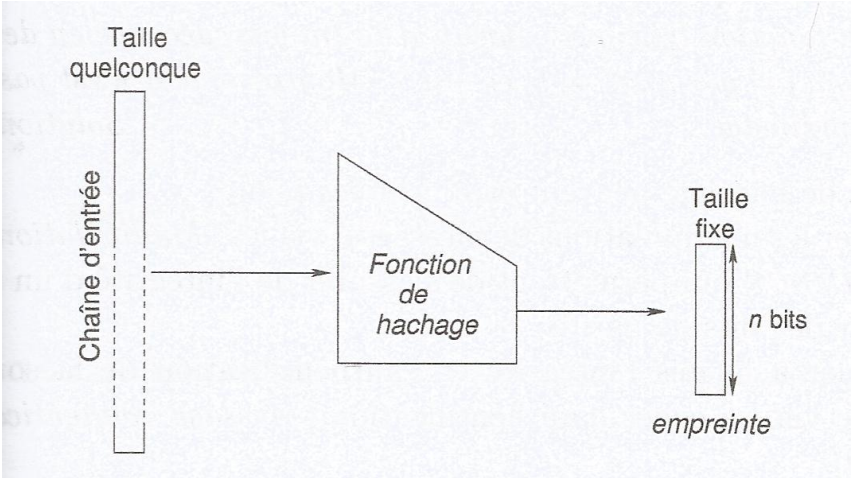
M2i M1 - CCI Avignon

17 septembre 2024

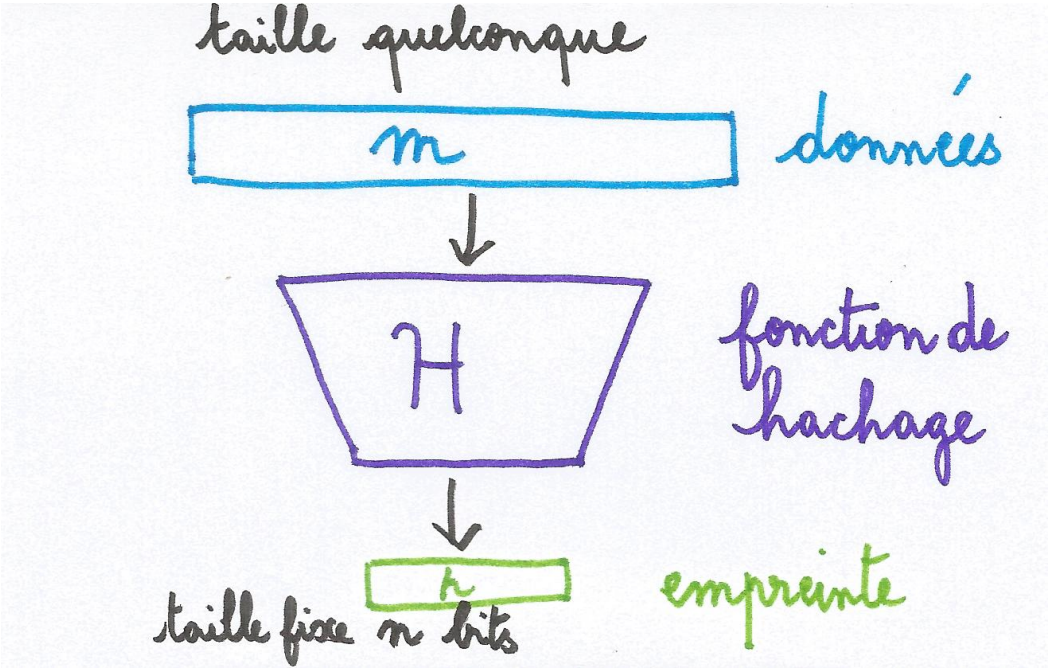
# Fonctions de hachage cryptographiques

message de longueur quelconque $\rightarrow$ valeur de longueur fixe

résultat = empreinte, haché, condensé, *digest*



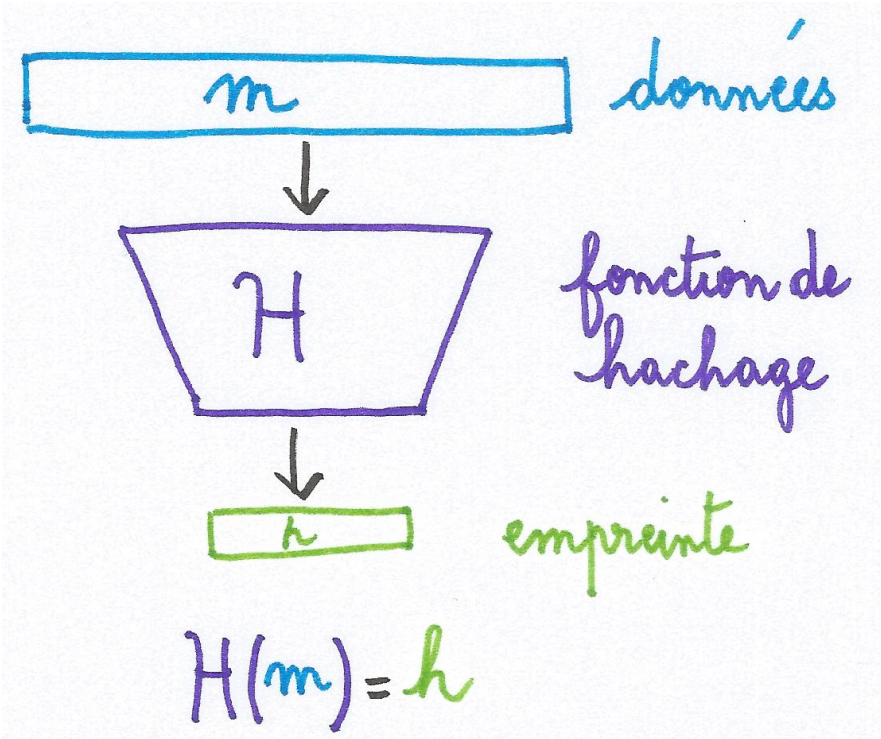
# Fonctions de hachages cryptographiques




taille des empreintes dépend de l'algorithme utilisé

# Collisions

$\mathcal{H}$ fonction de hachage




entrée de taille quelconque, sortie de taille $n$:

collisions inévitables

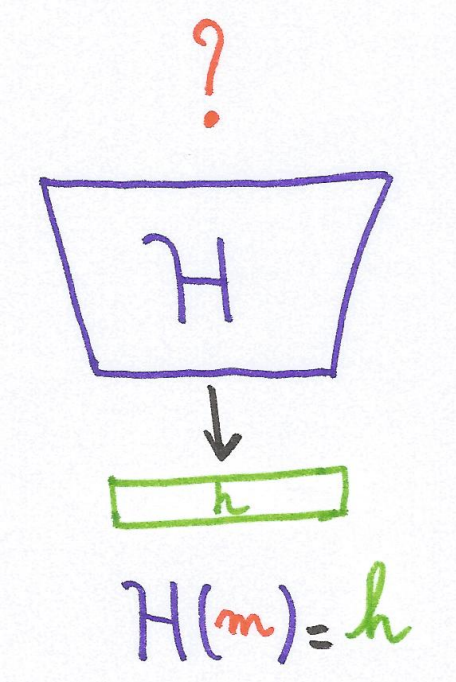
collision entre $m$ et $m'$ lorsque $\begin{cases} m \neq m' \\ \mathcal{H}(m) = \mathcal{H}(m') \end{cases}$

# Propriétés attendues

- $\mathcal{H}(m)$ doit être facile à calculer

- *résistance à la pré-image*:

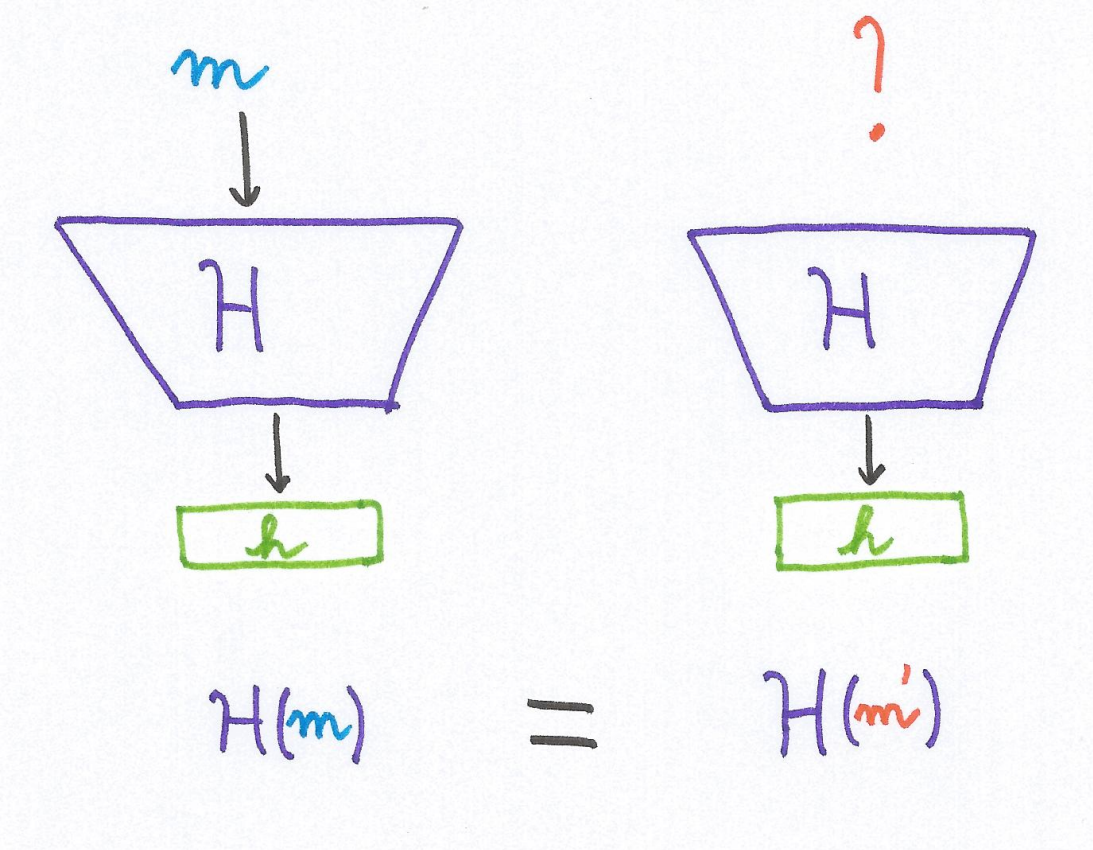
  étant donnée une empreinte $h$, il doit être calculatoirement difficile de retrouver un message $m$ tel que $\mathcal{H}(m) = h$



# Propriétés attendues

- *résistance à la seconde pré-image*:

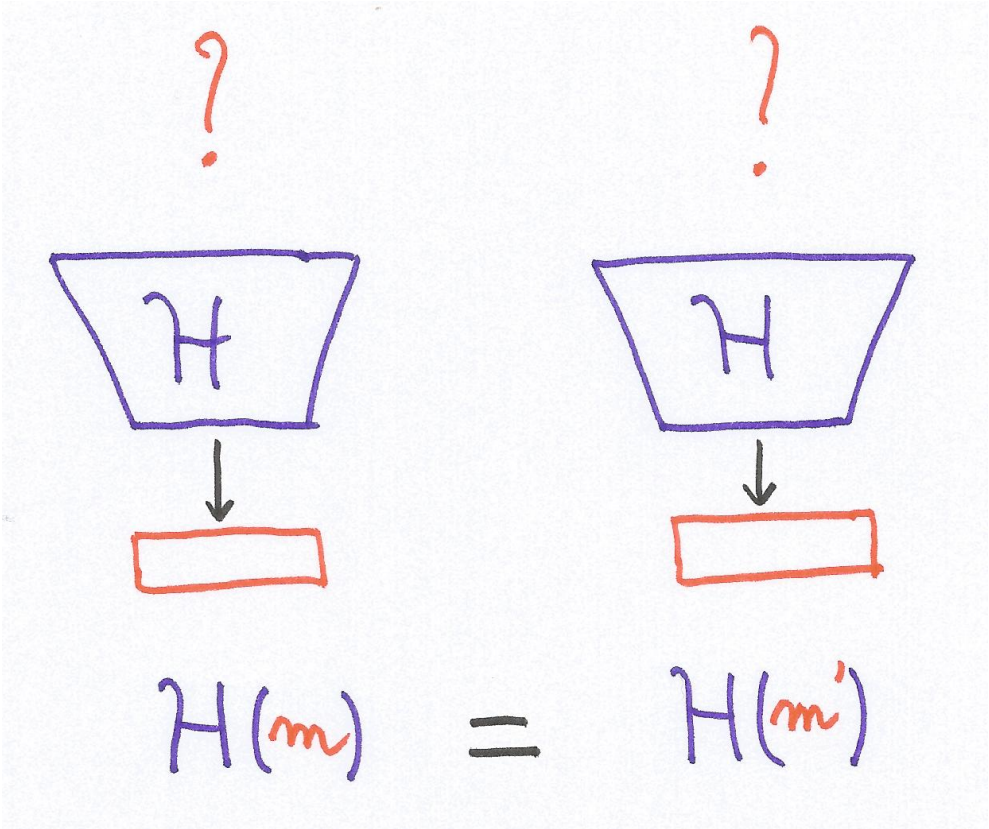
étant donné un message $m$, il doit être calculatoirement difficile de trouver un message $m'$ tel que $\mathcal{H}(m) = \mathcal{H}(m')$



# Propriétés attendues

- *résistance aux collisions*:

  il doit être calculatoirement difficile de trouver deux messages $m$ et $m'$ tels que $\mathcal{H}(m) = \mathcal{H}(m')$



# Fonctions de hachages cryptographiques

utilité:

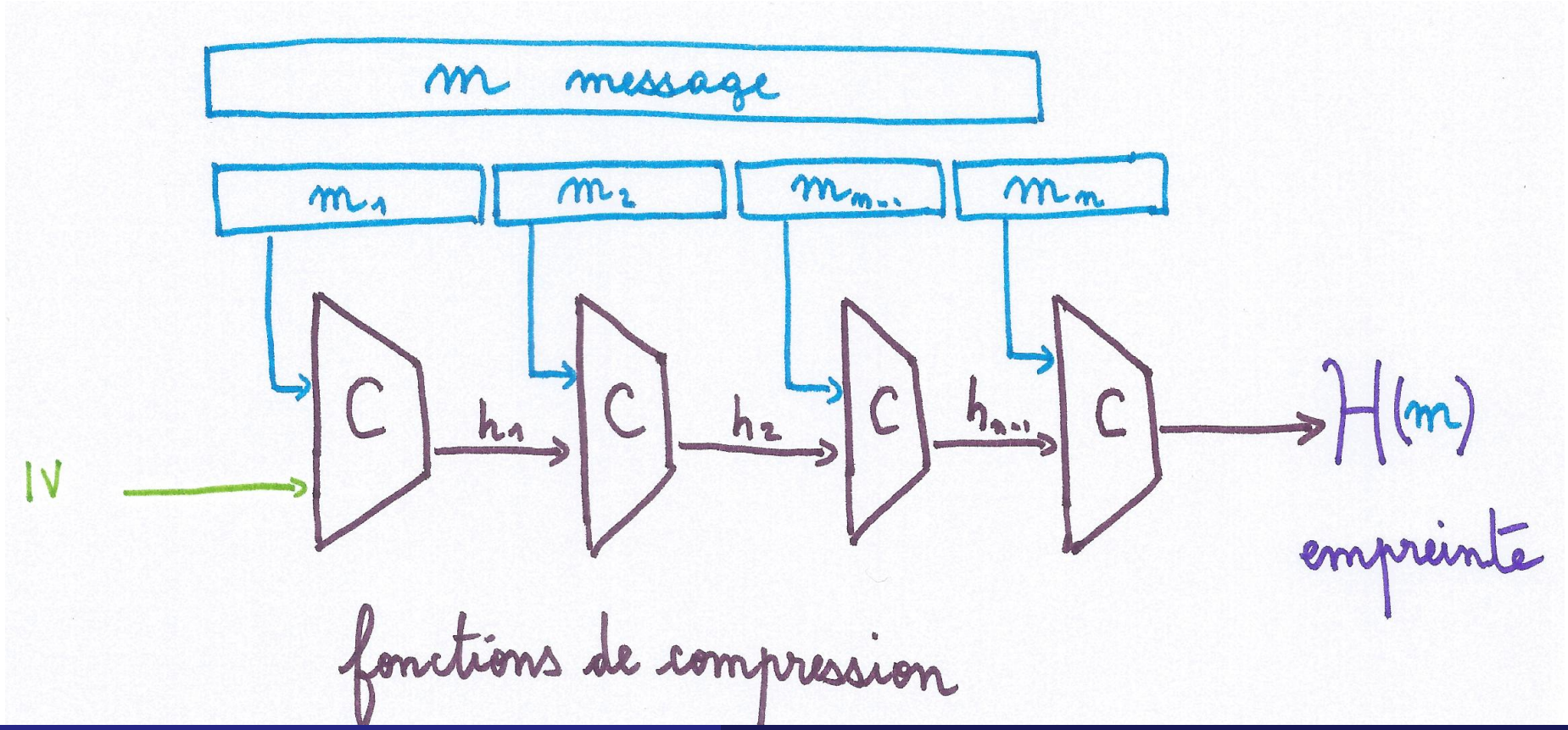
- vérifier l'intégrité d'un message
- vérifier l'authentification de la source

# Construction de fonction de hachage de Merkle-Damgård

message $m$ découpé en blocs de taille fixe (complétés) $m_1, ..., m_k$

itère une fonction de compression un certain nombre de fois.

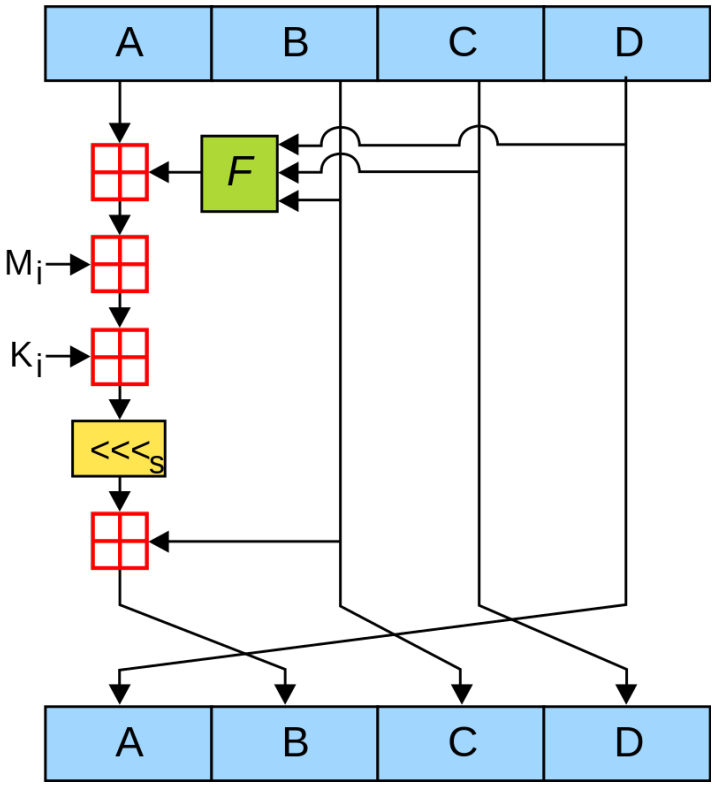
Un vecteur d'initialisation est utilisé pour le premier bloc.



# MD5 - *Message Digest 5*

1991 Ronald Rivest

Un tour: (il y a 64 tours)

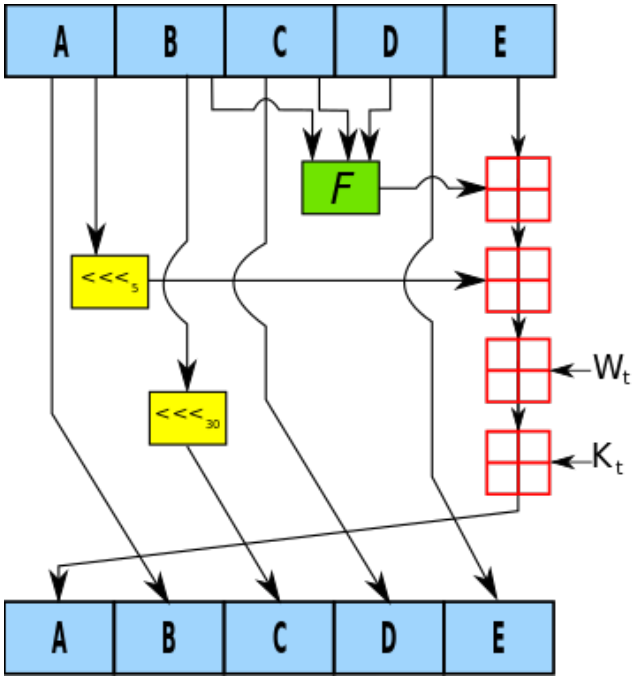



MD5 n'est plus considéré comme sûr aujourd'hui

longtemps utilisée

# SHA1- *Secure Hash Algorithm*

1995 National Security Agency - construction de Merkle-Damgård
message divisé en blocs de 512 bits
empreintes de 160 bits.
Un tour (il y a 80 tours):




SHA1 n'est plus considéré comme sûr.

# SHA2

famille de fonctions de hachage publiées en 2002

construction de Merkle-Damgård

SHA-256 et SHA-512

SHA-224 et SHA-384

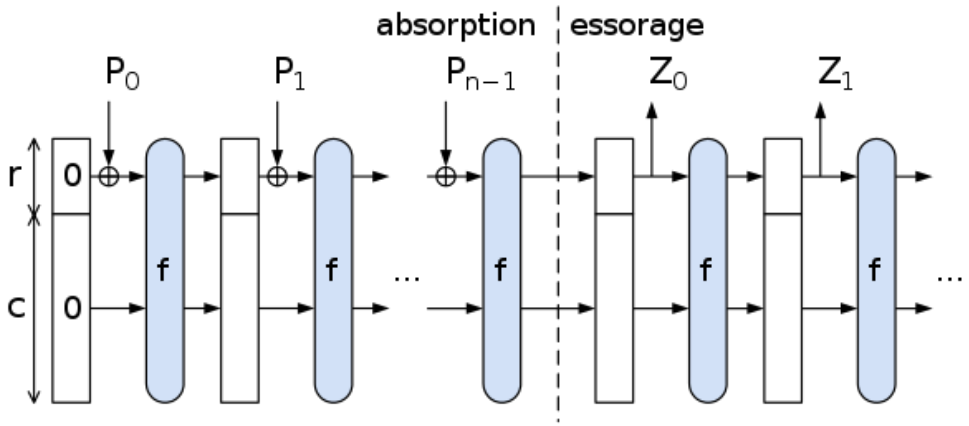
# SHA3

Keccak 2007

fonctions-éponges

entrée: chaines de taille quelconque

sortie: chaines de taille quelconque.



# hachage

```
anne@shuttle:~$ echo -n 'anne' | md5sum | awk '{print $1}'
e3fb62ebfa4f36acf5cbff6a6ed0f2e0
anne@shuttle:~$ echo -n 'a' | md5sum | awk '{print $1}'
0cc175b9c0f1b6a831c399e269772661
anne@shuttle:~$ echo -n 'anne anne' | md5sum | awk '{print $1}'
fe43481f288c3c67192a0b594e34d4a7
anne@shuttle:~$ echo -n 'anne' | sha1sum | awk '{print $1}'
96657fd33d4351fb0ec777fd7064e03b0adc3a35
anne@shuttle:~$ echo -n 'anne' | sha256sum | awk '{print $1}'
90b8de4051f02b7a29484341f3a903e1b2c6a233f5465e19c634535c7b315e6f
anne@shuttle:~$ echo -n 'anne' | sha384sum | awk '{print $1}'
fe54919fc1c2f51fa6804909de1b5c5da1d8808acb5666d66fea05078f9fa7d9f7e915a59dcdebf10382fa1ce43363af
```

# hachage

```
anne@anne-NS5x-NS7xAU:~$ echo -n 'Anne' | sha224sum |awk '{print $1}'
88ccf10ebd373146062a66b8bf4e6f583b32a7528182819855ee9368
anne@anne-NS5x-NS7xAU:~$ echo -n 'Anne'| openssl dgst -sha2-224|awk '{print $2}'
88ccf10ebd373146062a66b8bf4e6f583b32a7528182819855ee9368
```