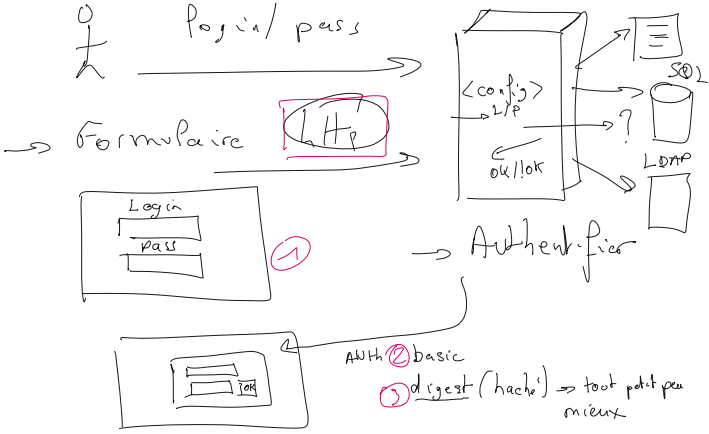
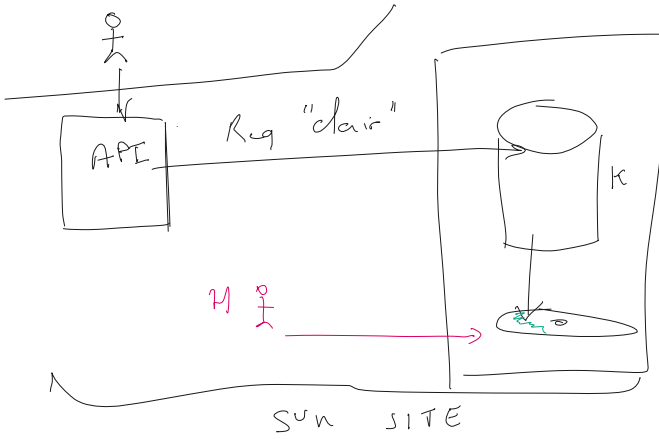
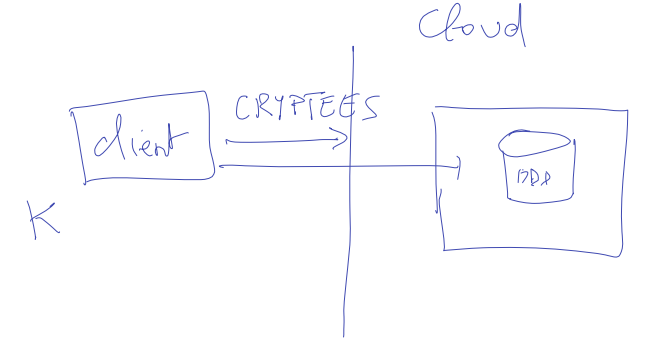


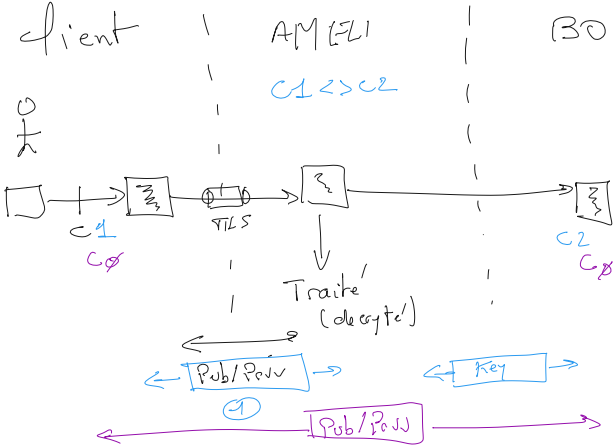

NTLM / Kerberos (4)

Login/mot de passe
(protocolatif)
Ancienne Techno

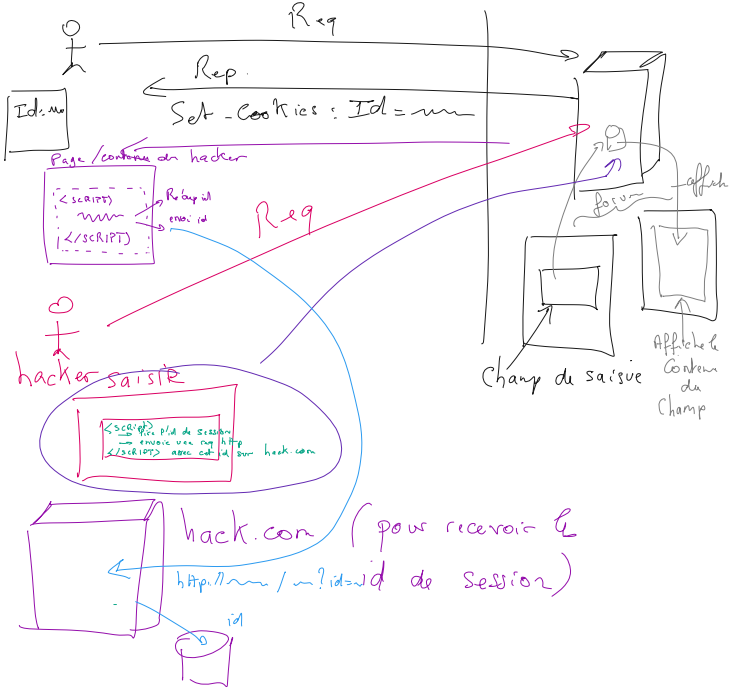
"Jeton"


API
Req "clair"
K
M
SUN SITE


Cloud
client
CRYPTEES
DATA
K


client
AMELI
BO
C1 <> C2
Ot
C1
C∅
TLS
C2
C∅
Traite'
(decrypte')
Pub/Priv
Key
Pub/Priv

# Exemple attaque XSS



Hash:

$f(Valeur_{entrée}) \rightarrow Valeur_{sortie}$

Collision

$f(v1) = f(v2)$

$v1 != v2$

1, 2, 3 = 6

1, 3, 2 = 6

→ Collision

MD5

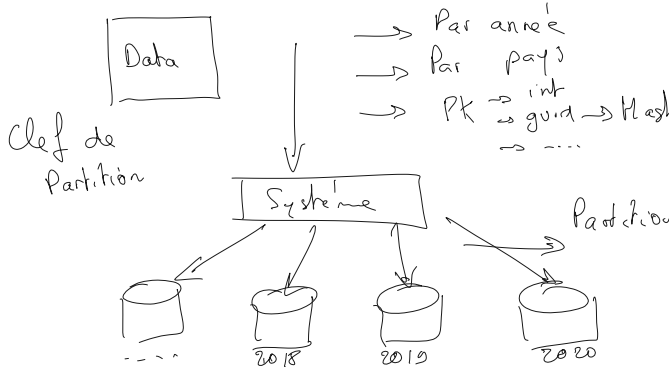
SHA (Ø) → 64 bits (8 octets)

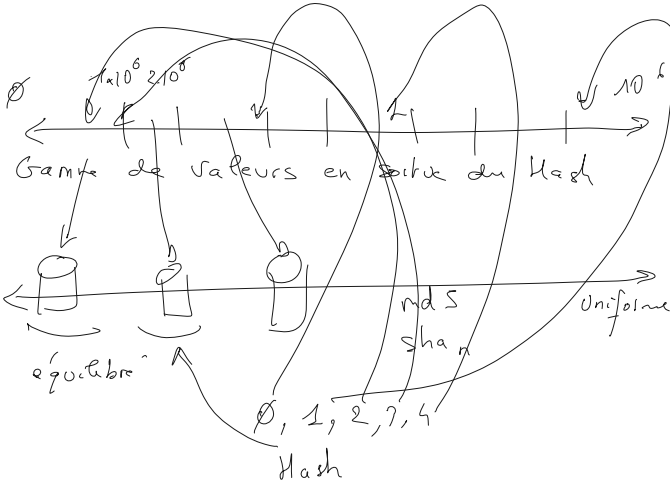
SHA1 → 128

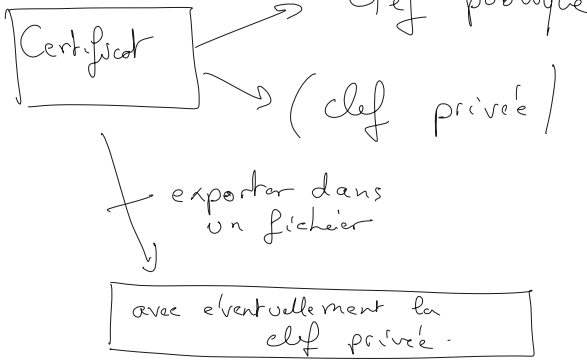
SHA2 → 256, 384, 512 ...

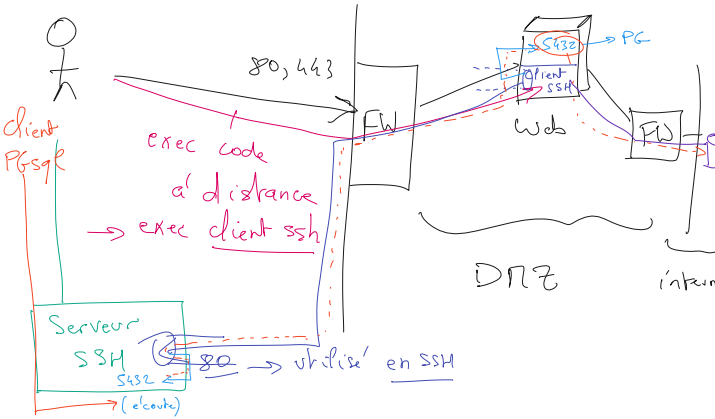
SHA3 → 1024, 2048 bits...

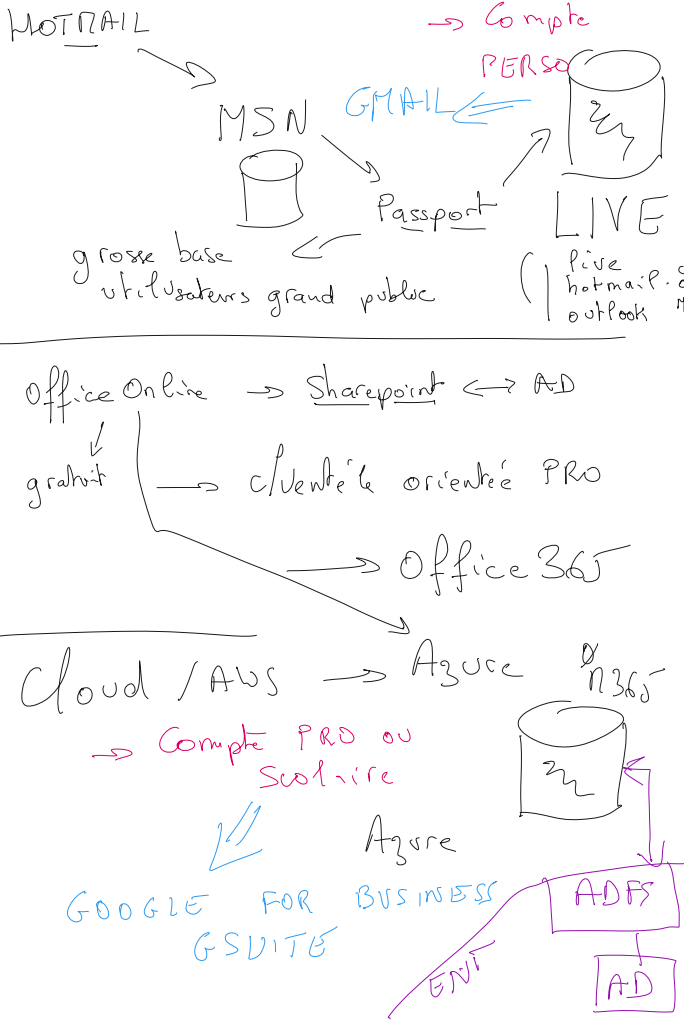
---




0
1*10^6
2*10^6
10^6
Gamme de valeurs en sortie du Hash
équilibré
rnd S
sha n
Uniforme
0, 1, 2, 3, 4
Hash


Certificat
clef publique
(clef privée)
exporter dans un fichier
avec éventuellement la clef privée.


80, 443
FW
client
PGsql
exec code
à distance
→ exec client ssh
5432
PG
client
SSH
Web
FW
DMZ
interne
Serveur
SSH
80
→ utilisé en SSH
5432
(écoute)


HOTMAIL
→ Compte PERSO
MSN
GMAIL
Passport
LIVE
grosse base utilisateurs grand public
live
hotmail.com
outlook
Office Online
→ Sharepoint ⟷ AD
gratuit
→ clientèle orientée PRO
→ Office 365
Cloud / AWS
→ Azure
O365
→ Compte PRO ou Scolaire
Azure
GOOGLE FOR BUSINESS
GSUITE
ADFS
AD
ENT