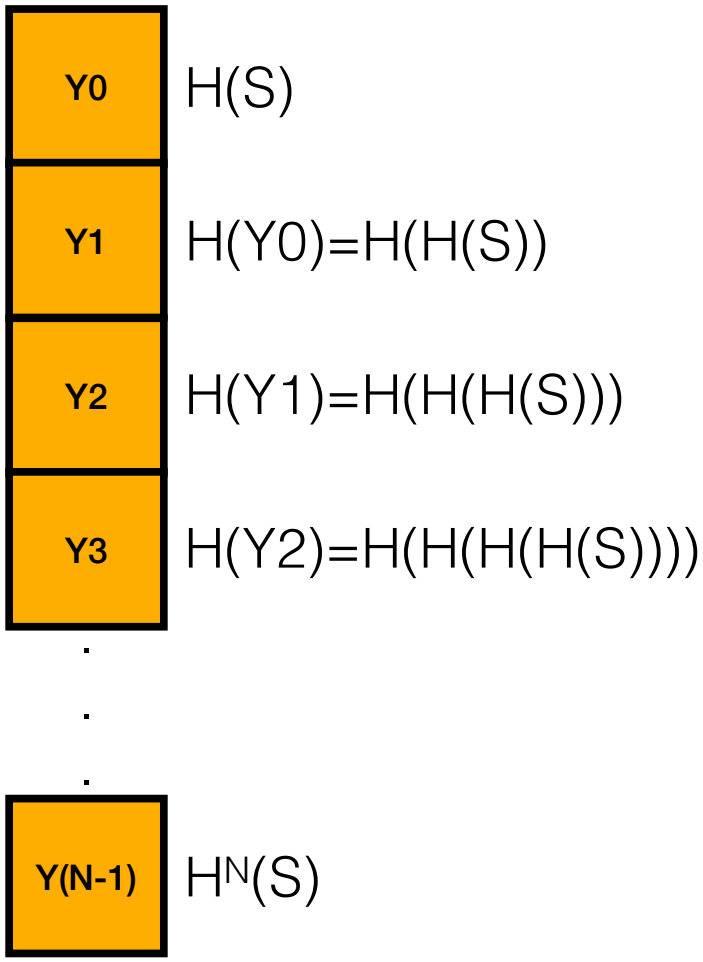
Scrypt

- Memory-hard function used in Litecoin, Dogecoin, …
- ASIC resistant (but it depends on how parameters are selected…)
- Used for password hashing



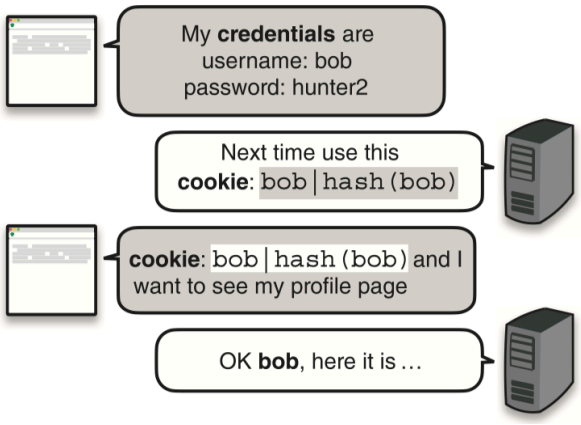
Scrypt:

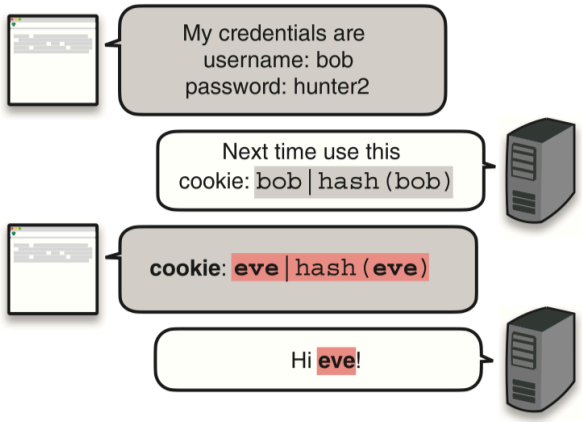
```
T=H(Y(N-1))
for i=0,…,N-1
  j=int(T) mod N
  T=H(T ⊗ Yj)
return T
```

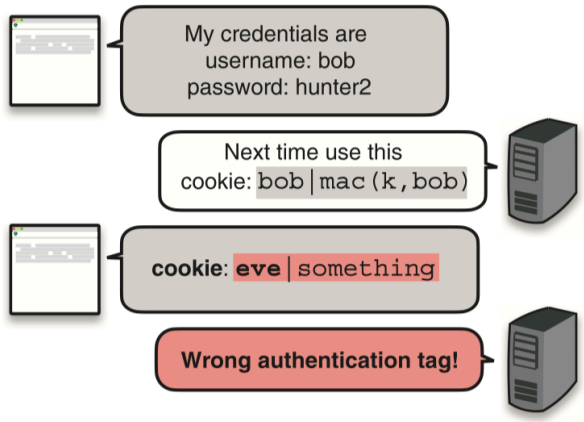
- Time/memory tradeoffs: store fewer Yi's and compute Yj from any Yi with i<j

- BAD as PoW: It is a password hashing scheme so verifier must perform same steps and use the same amount of memory

Message Authentication Codes (MAC)







From our textbook "Real-world Cryptography" by David Wong