S/KEY authentication OR Lamport's Scheme

- **ما هو؟:**
  - عبارة عن ألقوريثم يستخدم في عملية الـ Authentication بين الـ Client & Server
  - يصنف كنوع من أنواع الـ One-Time password
  - يعتمد على مفهوم الـ Hash chain
  - يستخدم في الـ OpenBSD و في بعض التقنيات الأخرى في linux
- **فكرته:**

الـ Cleint يقوم بتخزين الآتي :

  - دالة التشفير Encryption Function ولنرمز لها بـ **H(p)**
  - الـ **p** وهي عبارة عن النص الذي سيتم تشفيره
  - عدد معين نرمز له بـ **N** ، ويعبر عن عدد مرّات التشفير

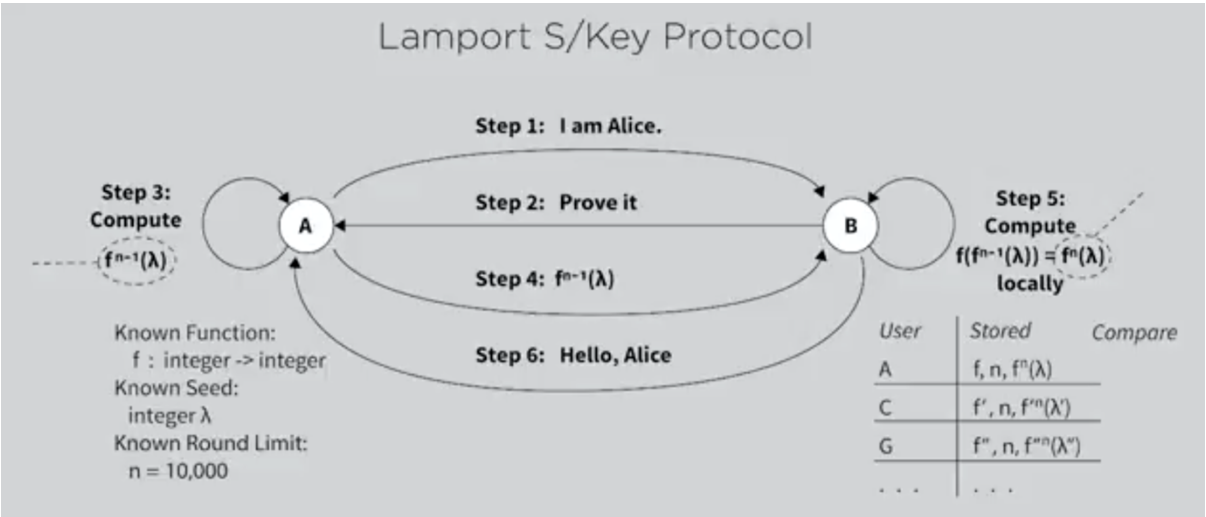
الـ Server يخزن الآتي:

  - دالة التشفير Encryption Function ولنرمز لها بـ **H(p)**
  - ناتج تشفير الـ p بعدد N من المرات ، أي يخزن المخرج من هذه الدالة $H^N(p)$
- **كيف يعمل؟:**

1- الـ Client يقوم بطلب الـ authenticate مع الـ Server
2- الـ Server يسأل الـ Client أن يُثبت هويته
3- الـ Cleint يقوم بحساب ==> $H^{N-1}(p)$ ويرسلها للـ Server
4- الـ Server يأخذ ناتج الـ $H^{N-1}(p)$ ويقوم بتشفيرها (مرة واحدة) بإستخدام دالة التشفير **H(p)** التي يملكها، ومن ثم يُقارن الناتج بالقيمة المحفوظة لديه مُسبقًا (التي هي $H^N(p)$) ، أي العملية تكون كالآتي:
$H(H^{N-1}(p)) == H^N(p)$?
5- إذا تساوت القيمتين من الخطوة 4 الـ Server يسمح للـ Client بالدخول، ومن ثم يقوم بتخزين قيمة $H^{N-1}(p)$ لديه
6- إذا طلب الـ Client الدخول مرة أخرى فإنه يقوم بحساب ==> $H^{N-2}(p)$ ويرسلها للـ Server
7- الـ Server يأخذ ناتج الـ $H^{N-2}(p)$ ويقوم بتشفيرها (مرة واحدة) بإستخدام دالة التشفير **H(p)** التي يملكها، ومن ثم يُقارن الناتج بالقيمة المحفوظة لديه مُسبقًا (التي هي $H^{N-1}(p)$) ، أي العملية تكون كالآتي:
$H(H^{N-2}(p)) == H^{N-1}(p)$?
8- إذا تساوت القيمتين من الخطوة 7 الـ Server يسمح للـ Client بالدخول، ومن ثم يقوم بتخزين قيمة $H^{N-2}(p)$ لديه

وبقية محاولات الدخول التي يجريها الـ Client تتم بنفس الخطوات السابقة

- الرسم التالي يلخص العملية:



- ملاحظات:
  - دالة التشفير **H(p)** من الممكن أن تكون أي One-way function مثل : **md4 , md5 , sha1 .. etc**
  - نلاحظ أنه في كل عملية authenticate بين الـ Client والـ Server ، الـ Server يجري **عمليتين** على القيمة التي استلمها من الـ Client وهما :
    1- حساب دالة التشفير لهذه القيمة
    2- تخزين هذه القيمة وإستخدامها في عملية المقارنة القادمة عندما يطلب الـ Client الدخول مرة أخرى

مرجع:
https://www.youtube.com/watch?v=zEgZrnvTYyI