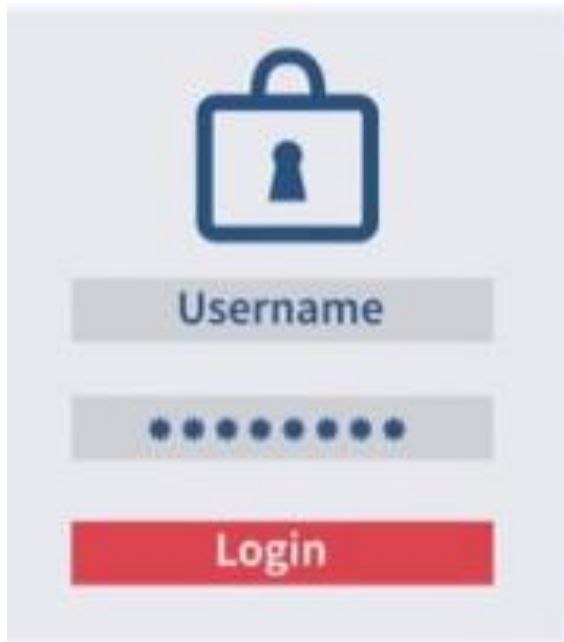




การสร้างความมั่นคง สำหรับหน้า Login ด้วย Mobile OTP

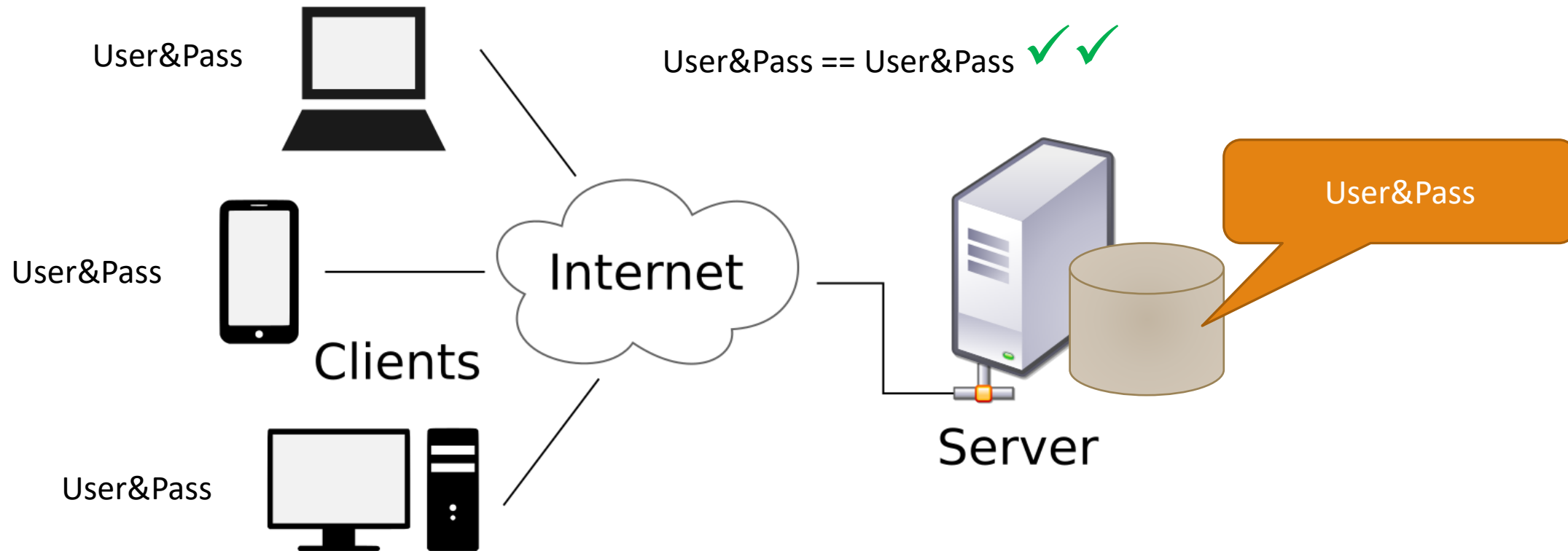
อ.ศราวุฒิ จันบัวลา

ล็อกอิน (Log in)



การเข้าสู่ระบบ ซึ่งสิ่งสำคัญที่ต้องใช้เข้าสู่ระบบก็คือ Username และ Password

การทำงานของ Login

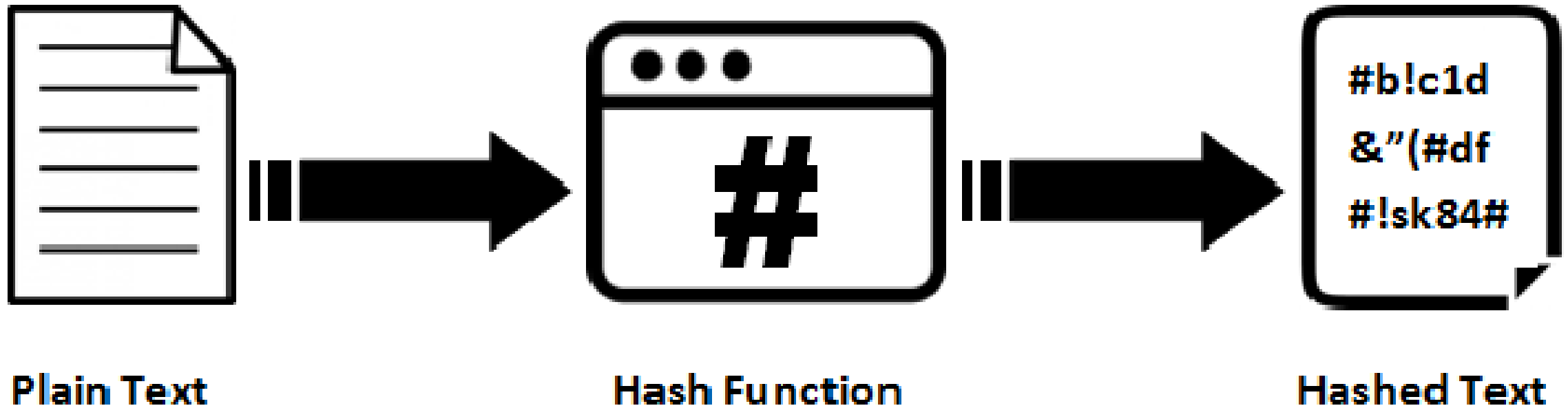


USERNAME	PASSWORD
USER1	PASSWORD1
USER2	PASSWORD2
USER3	PASSWORD3



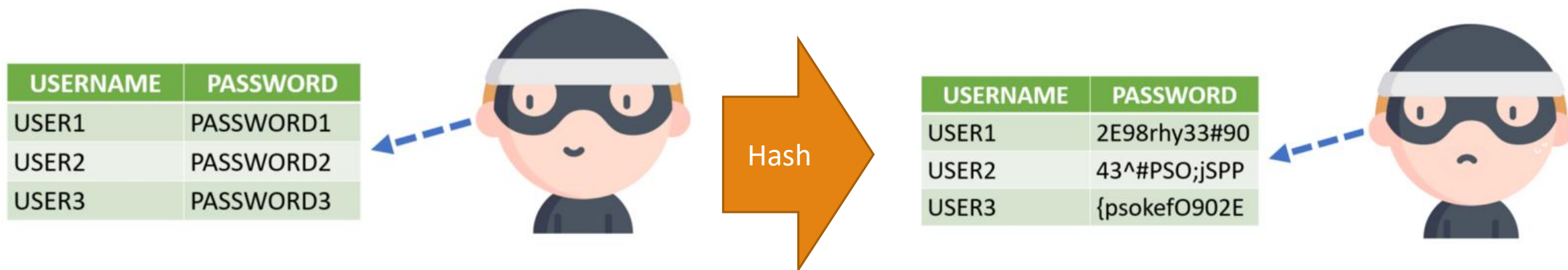
การจัดเก็บ User และ Pass

Hashing Algorithm



Hash Algorithm

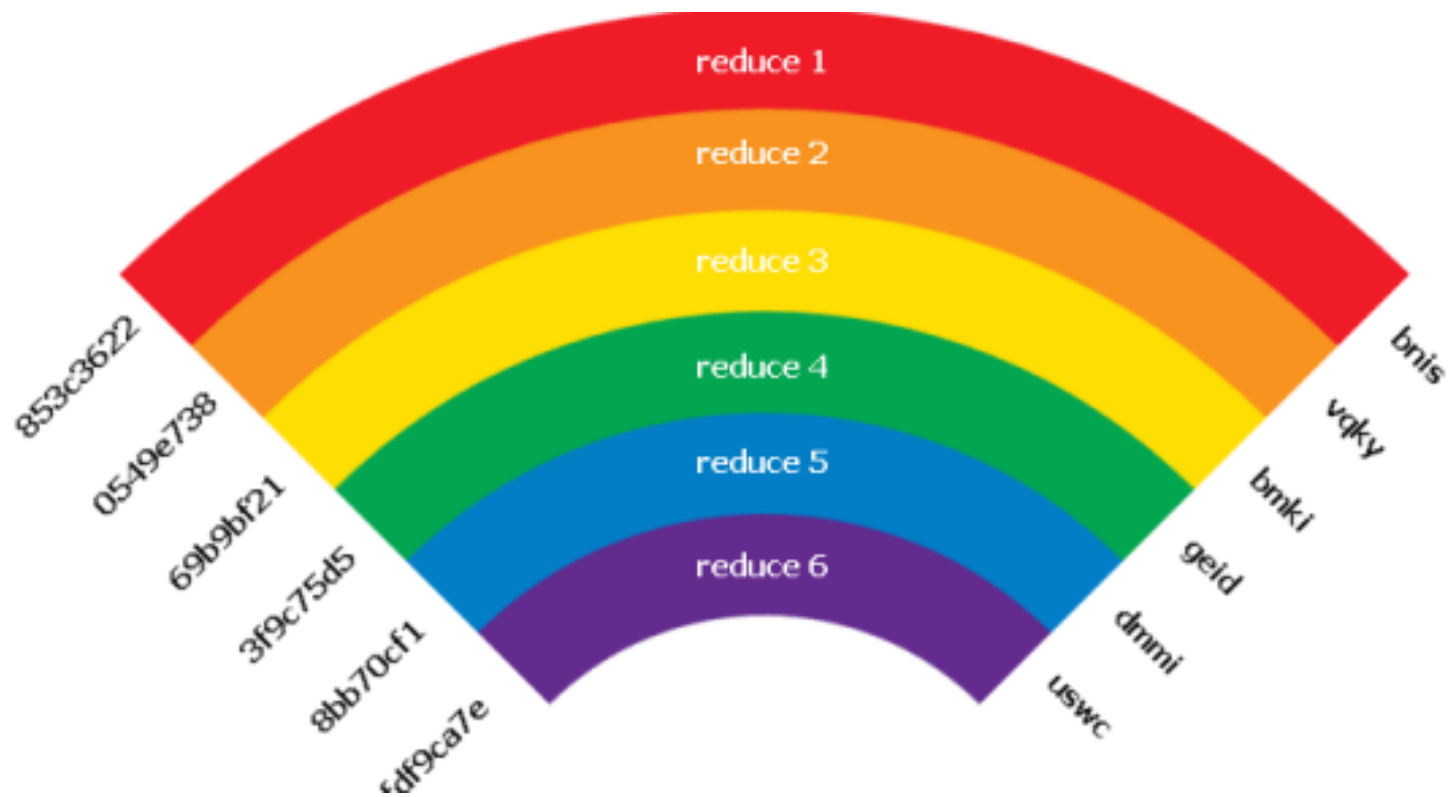
การเก็บรักษา Password ด้วย Hash Function



<https://crackstation.net/>



Brute Force

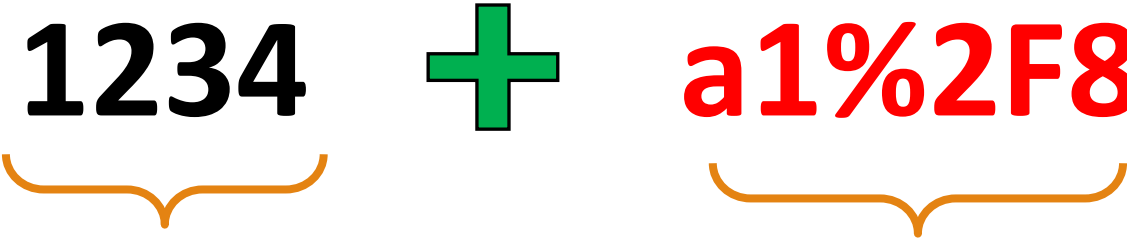


RainbowCrack

เพิ่มความแข็งแกร่งให้กับ Password ด้วย Salt

คืออักษรที่ถูกสุ่มขึ้นมาเพื่อเพิ่มความยากกับ พวก wordlist

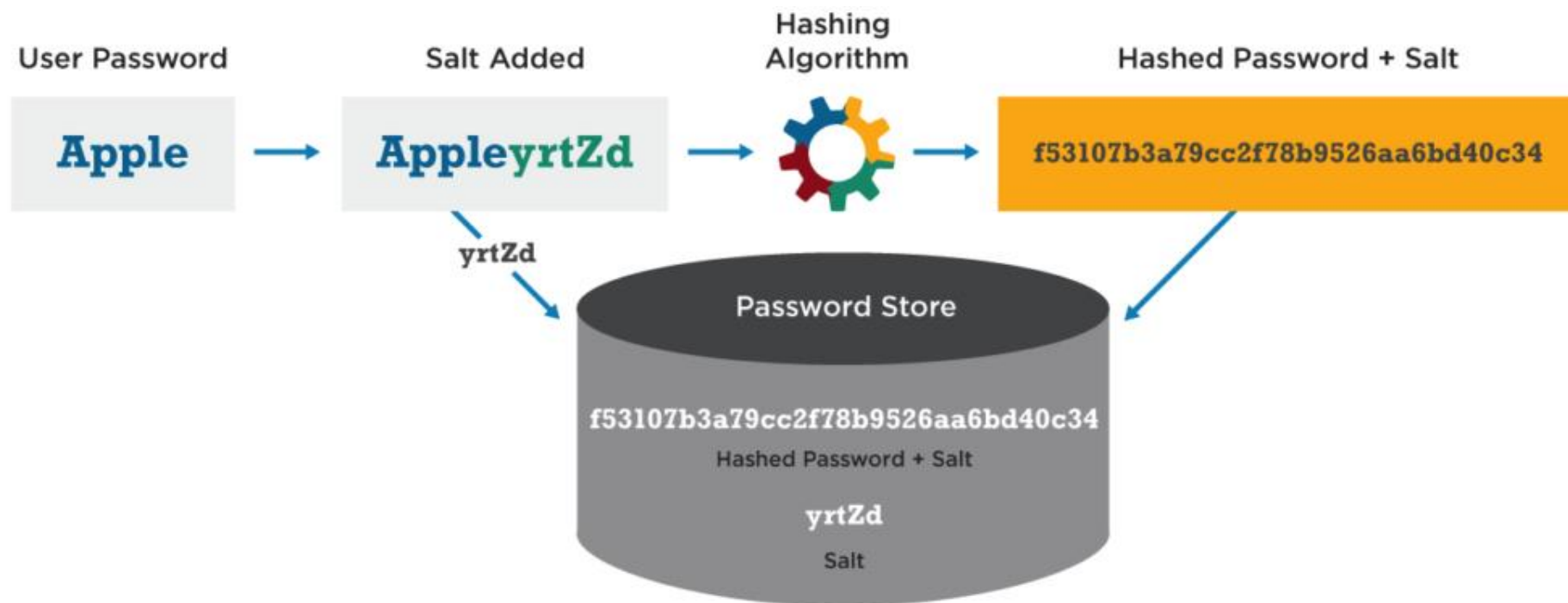
1234 + **a1%2F8**



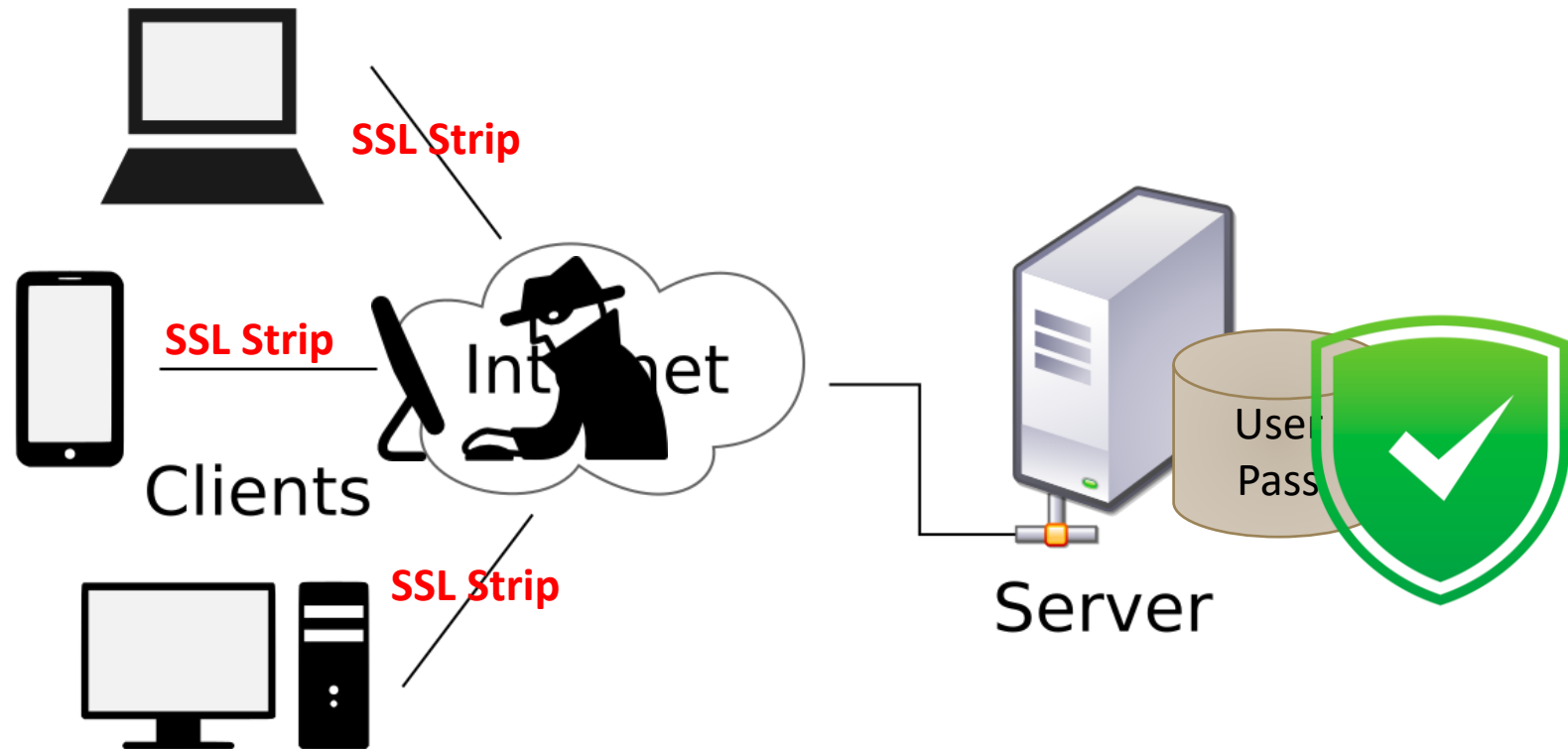
Password Salt

1234a1%2F8

การจัดเก็บ Password และ Salt



SSL Stripping

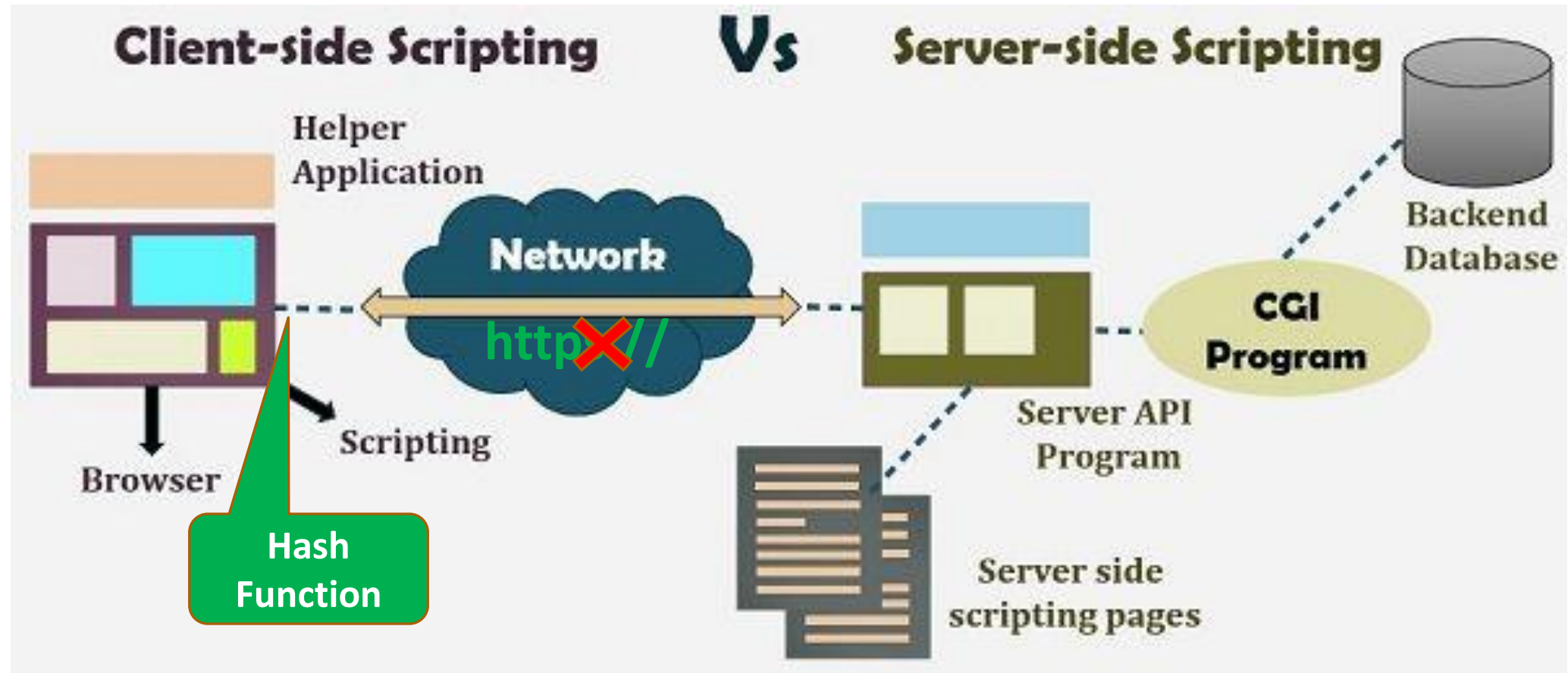




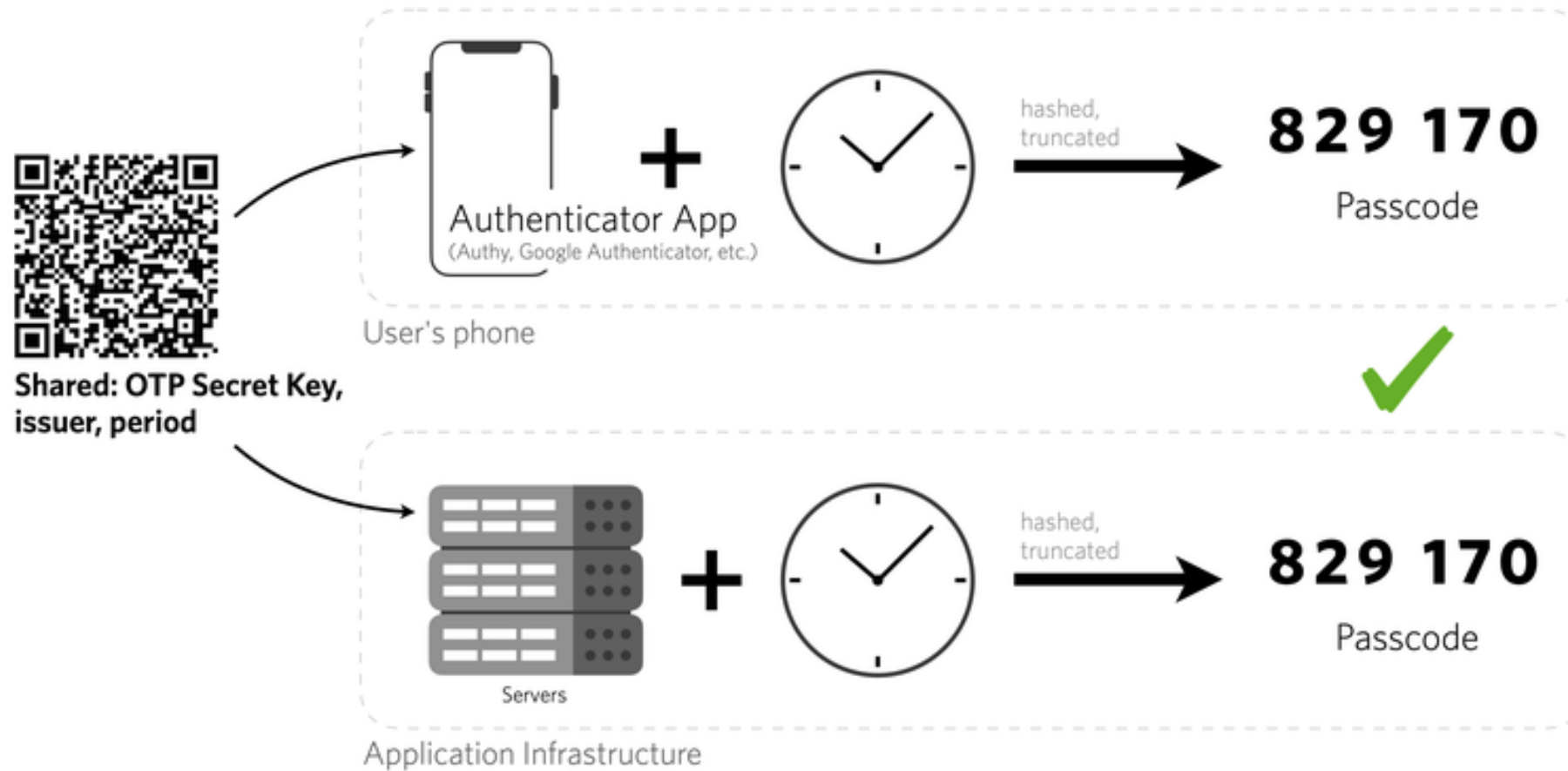
**NOT
SECURE**



JavaScript Bodyguard

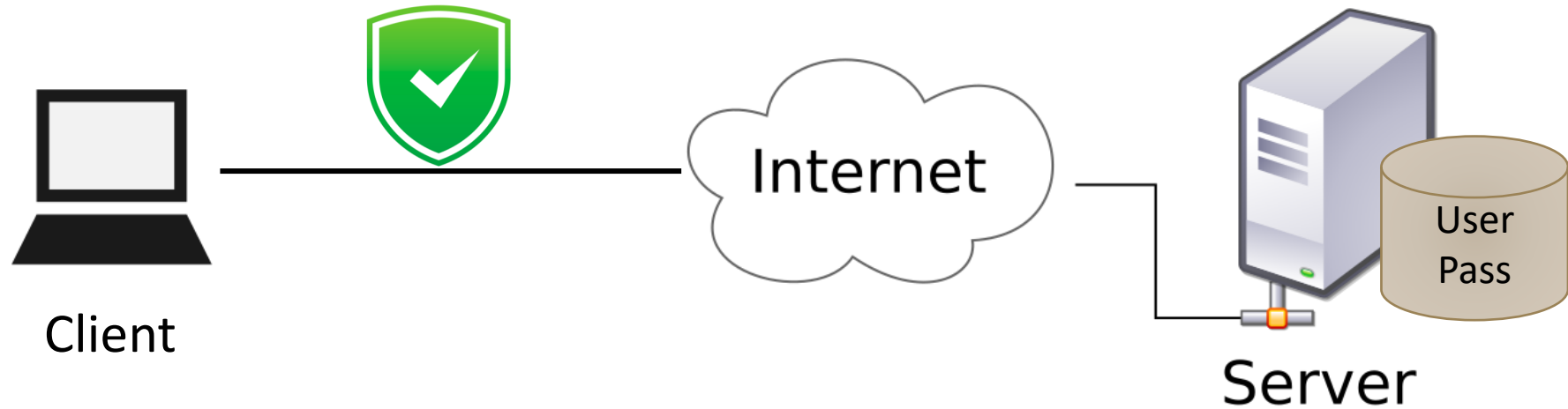


TOTP algorithm



การสร้างมั่นคงให้กับหน้า login

Hash + Mobile TOTP



Username

User



hash(User)



hash(hash(User))



e63648d6fb6cc5389fb03ce44597010b7e179bfd881a5223a6df29ddd5034b5f

Password

Pass



hash(Pass)



hash(hash(Pass))



hash(hash(hash(Pass))+OTP)



ea7f237e57e481fc2ad4301d69b74da7d1d586675a66065167f7dd783ac92a50

Web+Mobile OTP

Web => <https://www.isanmsu.com/bank/>



Login to ISAN Bank





[Forgot Username/Password?](#)

Login

This is not a real online banking.
It is just a test-bed to test & demo,
how to protect against bank hacking.

Mobile OTP



shorturl.at/acdJY