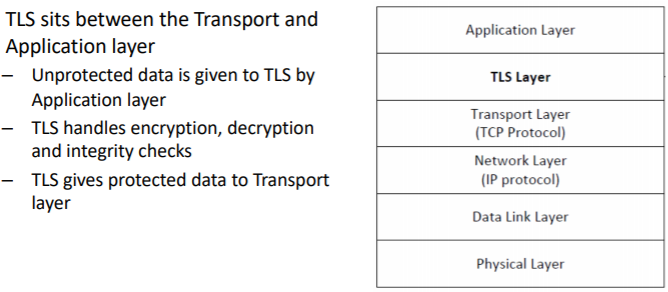
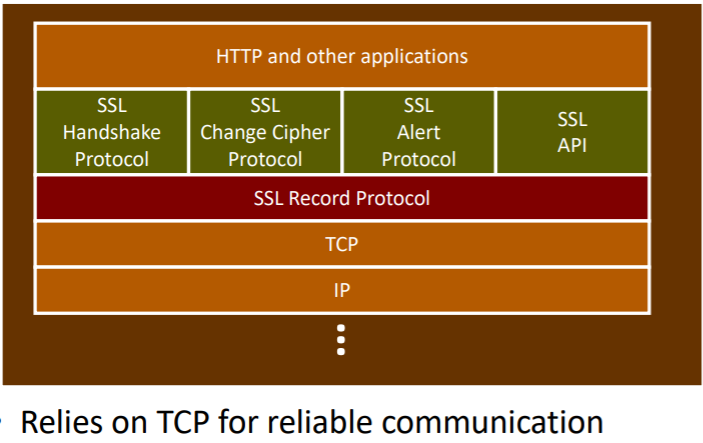
TLS:



SSL:



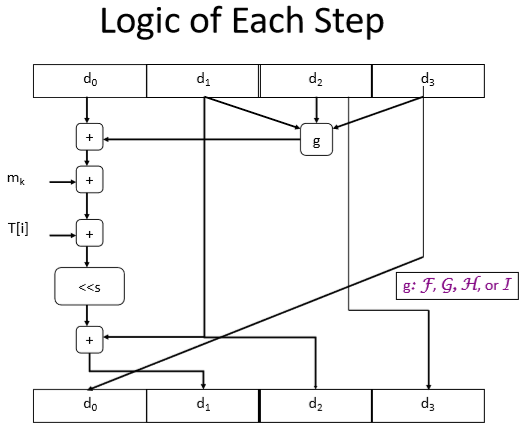
TLS is a protocol that provides a secure channel between two communicating apps:

Confidentiality: Nobody other than the two ends of the channel can see the actual content of the data transmitted

Integrity: Channel can detect any changes made to the data during transmission

Authentication: At least one end of the channel needs to be authenticated, so the other end knows who it is talking to.

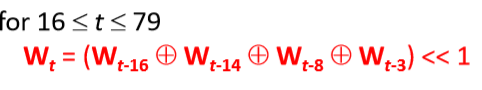
MD5 Hash missing:



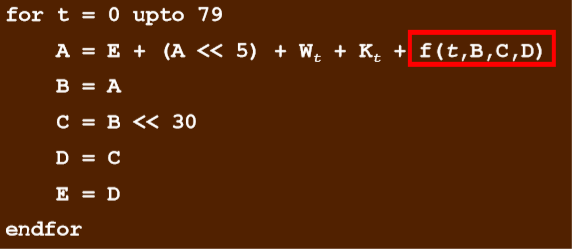
SHA-1 algorithm:

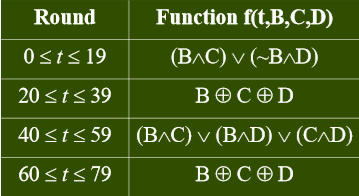
Let 512-bit block be denoted as sixteen 32-bit words W0..W15

IV: A= 0x67452301, B= 0xEFCDAB89, C= 0x98BADCFE, D= 0x10325476, E= 0xC3D2E1F0



For t < 16 , use W0..W15 from the input

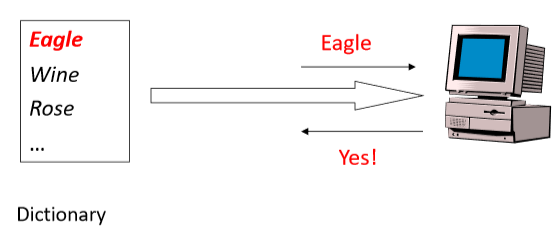




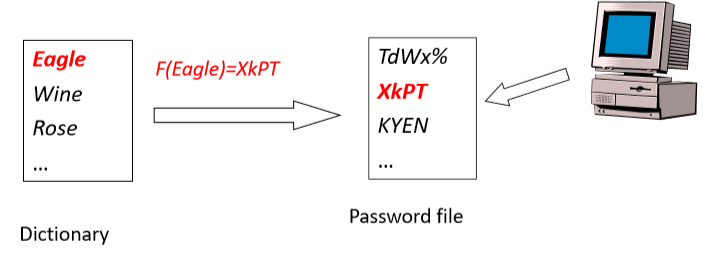
Output (t = 79) is added to input of first step (t = 0) to produce 160-bit Message Digest (A + B + C + D + E)

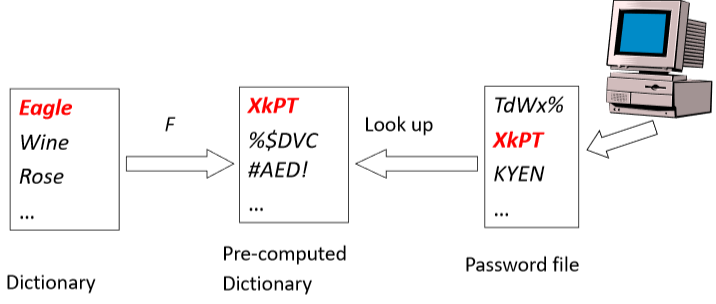
Dictionary Attack:

Online



Offline



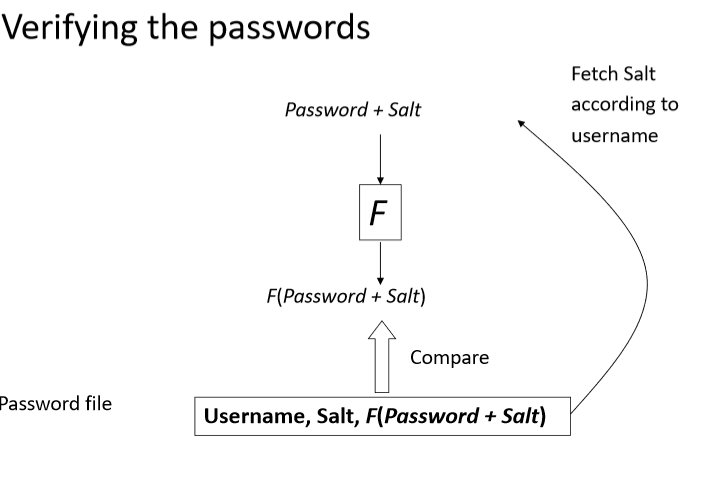


Password Salt:

+Prevent dictionary attack

+salt is a n-bit number between 0 and 2^n

+derived from system clock and the process id



IP vulnerabilities:

Port Scanning: ports dynamically address (“bind”) IP packets to a process

solution: scan for open ports that do not need to be accessible from outside =>block them/shut them down

OS fingerprinting:

Solution: use a virtual machine when access outside network

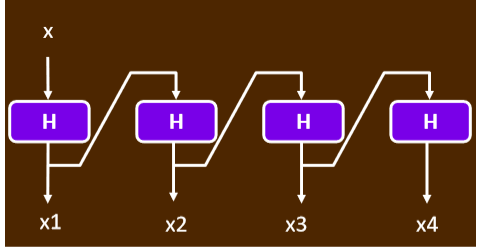
IP spoofing:

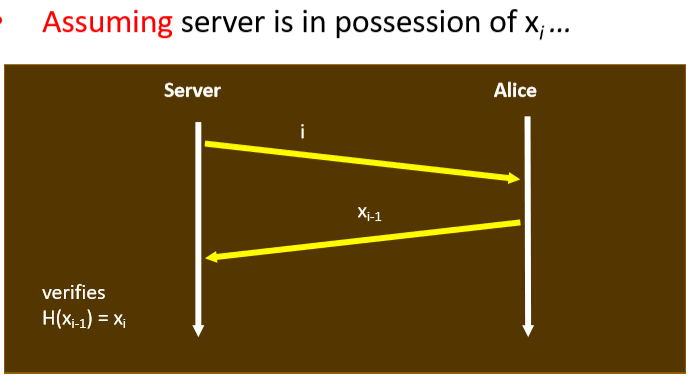
* Router filtering

S/key (Lamport’s Hash)

User selects a password x and generates n number of passwords

Key feature: no one knowing xi can easily find an xi-1 such that H(xi-1) = xi (only user knows)





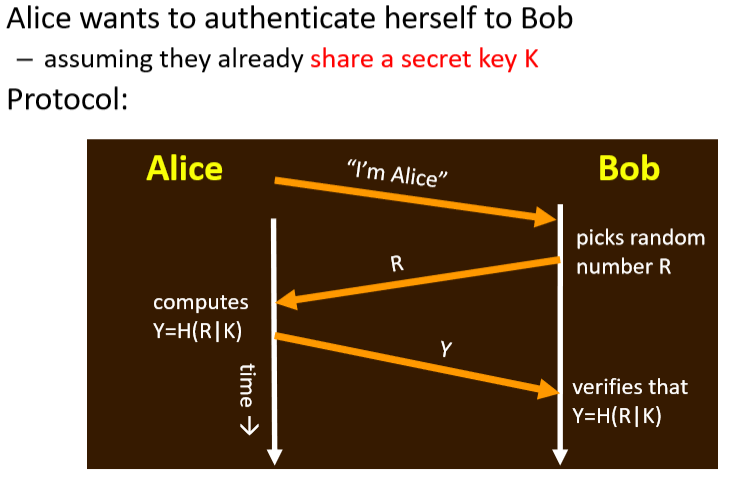
Limitations:

+periodically regenerate a new chain of passwords

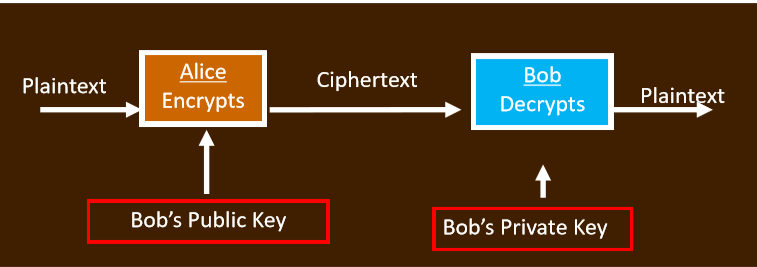
+Cannot authenticate server. (middle man attack can happen, a fake server can get trick user to give the hash, which will send to the real server)

User Authentication:

Using hash function:



Using public and private key pair:



Can be based on:

Password-based authentication (dictionary attack)

Address-based user authentication (network address spoof)

Crypto-based authentication