Week-09 SSH + Crypto-1

**1. Explain conceptually all the following terms, and how/why they are needed for SSH and TLS/SSL**

* **Symmetric Encryption**

En krypteringsform der skal bruge en nøgle til at kryptere og dermed samme nøgle til at dekryptere.  Dette skaber dog et problem når nøglen skal uddelegeres. I dét der også kun er en nøgle er der også en risiko for at man mister nøglen eller at en uvedkommende får adgang til den, og derved har mulighed for at dekryptere alt informationen.

* **Asymmetric Encryption**

En krypteringsform, som differentierer sig fra den symmetriske kryptering ved at have krav om to sammenhængende nøgler, for at kunne sende data - en private key og public key. Eftersom de to nøgler er forbundet med hinanden skal det noteres at det ikke er muligt at få fat i private key gennem public key, hvilket er yderst vigtigt da public key frit kan deles med hvem som helst. Forholdene mellem de to er banalt at public key krypterer beskeder, som kun den associerede private key kan dekryptere.  
Dette er en ‘ensrettet vej’, så det vil ikke være muligt for en private key at kryptere en besked til dens public key(s). Eftersom private key er den eneste måde at dekryptere de associerede public keys, er det et absolut krav ikke at dele private key.

Eksempel: SSH benytter sig af asymmetrisk kryptering på forskellige punkter. Ved udvekslingen af nøgler til symmetrisk kryptering. Her bliver der lavet midlertidige nøgler for at kunne producere ‘shared secret’ som bruges i symmetrisk kryptering. Ydermere bliver asymmetrisk kryptering også brugt ved eksempelvis autentificere en brugers adgang til en server.

* **Hashing**

En hashfunktion er en funktion der omdanner information til en mindre

værdi. Dette er dog en envejs funktion, så man kan ikke omdanne mindre

information til det originale information. Man kan ikke gå den anden vej.

Den skulle meget gerne være unik (ingen kollisioner), selvom der ikke er

nogen matematik garanti for at den bliver det.

Hashing har den modsatte måde at kryptere og dekryptere som asymmetrisk kryptering, ved det skal det forstås som at krypteringen sker i gennem private key, som derved giver en digital signatur så man kan se hvem afsenderen er. Public key er så den der bliver brugt til at dekryptere.

(F.eks. MD-5 og sha-256)

**2. Explain what it takes to safely log in to an SSH server, without having to provide a password**

Det for at etablere en sikker SSH forbindelse imellem klient og server er det første skridt at oplyse serveren om klients (klient der skal kunne have adgang til at SSH i serveren) public key. Derefter kan man tilgå serveren, og første gang man gør det får man også tildelt en public key fra serveren. Der er nu etableret en sikker forbindelse mellem de to parter. Dog skal serverens public key ændres gang til gang, ellers kan der opstå man-in-the-middle attacks (kan ikke huske hvorfor though).

**3. Explain the term SSH-tunnel, and provide a practical example for its use**

**4. Explain conceptually the purpose of Symmetrical Encryption, Asymmetrical Encryption and hashing for an SSH-connection**

Et problem ville opstå hvis man brugte symmetrisk kryptering til forbindelser mellem 2 parter, da man overføre en key for dekryptering. Dette problem bliver løst af asymmetrisk kryptering.

**5. Explain the steps you have to go through to setup a server with MySQL,  as secure as possible →**

* **How can we limit the client IP's that can connect**
* **If set up to allow only localhost and a firewall that deny 3306, can we still connect “safely” from a remote server**
* **how to set up an SSL connection that  anyone can use,**
* **Demonstrate a client application (Java or whatever you prefer) running on a separate server that access the Database using SSL**