Opgave 28

1. Der er typisk fire ting, man gerne vil opnå med net sikkerhed –nævn de fire ting.  
   - Fortrolighed: Andre må ikke kunne se data  
   - Beskedintegritet: Andre må ikke kunne ændre på data  
   - Autentifikation: Man ved, hvem modtager/afsender er  
   - Operationel sikkerhed: Systemerne og netværket holdes kørende
2. Hvilken af de fire ting vil en god kryptering sikre?  
   -En god kryptering vil sikre fortrolighed.
3. Hvad er den væsentligste fordel og de væsentligste ulemper ved symmetrisk kryptering?  
   - Den væsentligste fordel ved symmetrisk kryptering er hastighed og effektivitet, men ulemperne er, at nøgler skal deles sikkert, og at der kan opstå problemer, hvis en nøgle går tabt eller bliver kompromitteret.
4. Hvad er den væsentligste fordel og de væsentligste ulemper ved public keykryptering?  
   - Den væsentligste fordel ved public key kryptering er, at det eliminerer behovet for at dele nøgler sikkert. Ulemperne er, at det er langsommere og mere beregningsmæssigt krævende end symmetrisk kryptering.
5. Hvilken nøgle bruges når man vil kryptere med public key kryptering?  
   - Når man vil kryptere med public key kryptering, bruger man modtagerens offentlige nøgle.
6. Hvilken nøgle bruges når man vil dekryptere med public key kryptering?  
   - Når man vil dekryptere med public key kryptering, bruger man sin egen private nøgle.
7. Hvordan kan man sikre message integritet?  
   - Man kan sikre message integritet ved at bruge en hash-funktion til at generere en hash-værdi for meddelelsen og derefter inkludere denne hash-værdi i meddelelsen eller ved at anvende digitale signaturer.
8. Hvad er forskellen på de hash-funktioner man bruger til at opdage transmissionsfejl og de hash-funktioner, der anvendes til message integritet?  
   - Hash-funktioner, der anvendes til at opdage transmissionsfejl, er normalt simple og hurtige, mens hash-funktioner, der anvendes til message integritet, er mere komplekse og kryptografisk sikre.
9. Hvad sikrer en digital signatur?  
   - En digital signatur sikrer autenticitet og integritet af en meddelelse.
10. Hvad bruger man når man laver en digital signatur?  
    - Når man laver en digital signatur, bruger man sin private nøgle til at kryptere en hash-værdi af meddelelsen og inkluderer denne i meddelelsen.
11. Hvad er et CA og hvad gør det godt for?  
    - Et CA (Certificate Authority) er en tredjepart, der udsteder digitale certifikater og sikrer, at de er gyldige og autentiske.
12. Hvad er et certifikat?  
    - Et certifikat er en digital signatur udstedt af en CA, der bekræfter autenticiteten af en offentlig nøgle eller en persons identitet.
13. Hvad er replaying og hvordan er det farligt?  
    - Replay-angreb er, når en hacker optager og genafspiller en tidligere transmission for at opnå uautoriseret adgang. Dette kan være farligt, da det kan føre til manipulation af data eller uautoriseret adgang til systemer eller netværk.
14. Hvordan kan man sikre mod replaying?  
    - Man kan sikre mod replay-angreb ved at bruge timestamping, sequence numbering eller nonce til at identificere og afvise genafspillede meddelelser, samt ved at bruge kryptografiske teknikker som HMAC eller digitale signaturer til at verificere meddelelsens integritet og validitet.

Opgave 29

Denne opgave er en meget kort repetitionsopgave i netsikkerhed. Du skal binde nedenstående tal sammen med nedenstående bogstaver.

1.Fortrolighed 🡪 B

2.Beskedsintegritet. 🡪 E

3.Digital signatur 🡪 C

4.Certifikation Authority 🡪 A, **F**

5.Autentifikation 🡪 G, H

6.TLS 🡪 D, I

A. TDC er et eksempel på dette

B. Kan sikres alene med kryptering

C. I dette begreb indgår både at teksten ikke er ændret og man ved hvem, der har signeret det.

D. Fortrolighed og beskeds integritet sikres af denne mekanisme

E. SHA 1 og MD5 er teknikker, der ofte anvendes til at sikre dette

F. Skal sikre at man kan stole på hvem der har en bestemt public key

G. Findes tit omtalt både som client-og server-.

H. Begrebet dækker at man ved, hvem det er man kommunikerer med

I. Den service, der anvendes af HTTPS