TTM4135 kontinuasjonseksamen 16.august 2005 - løsningsskisse

1. Autentisering – å vise at kommunikasjonen er autentisk, dvs. korrekt og komplett mht. avsender og innhold.
2. Asymmetrisk kryptosystem – kryptering med en offentlig sendernøkkel, og dekryptering med en hemmelig mottakernøkkel.
3. Digitalt sertifikat – digitalt signert melding som vanligvis kobler navn/identitet og offentlignøkkel autorativt.
4. Datavirus – Programkodetillegg som kopierer og skriver seg selv til andre programfiler, og kan forårsake annet skadeverk.
5. Dataorm – Hærverksprogram som er distribuert over flere vertsmaskiner, og som kommuniserer og replikerer/ekspanderer over datanett.
6. HMAC- standard algoritme for å generere meldingsautentiseringskode, basert på enveis hash funksjon. ”Keyed-Hashing for Message Authentication”
7. Informasjonsteoretisk sikker – også benevnt perfekt sikkerhet, dvs. informasjonsbeskyttelsen er uavhengig av beregningsmessig kapasitet hos motstanderen.
8. Nonce – et tall eller kode som benyttes en og bare en gang.
9. X.509 – en ITU-T anbefaling for autentisering i katalogtjenester X.500, inkl. ”standardformat” for digitalsertifikat.
10. Gjentaksangrep – kommunikasjon basert på å repetere/duplisere en allerede gjennomført autorisert kommunikasjon.
11. SNMP MIB – Simple Network Management Protocol Management Information Base inneholder sikkerhetsparametere.
12. ISAKMP – Internet Security Association and Key Management Protocol, del av IPsec standarden.
13. PGP – Programvare for offentlignøkkel kryptografitjenester for filer og epost.
14. Kerberos – distribuert system for autentisering av brukeraksess til vertsmaskintjenester.
15. S/MIME – Secure/Multipurpose Internet Mail Extension, et sikkerhetstjenestetillegg til Internet epoststandard dokumentert i IETFstandarder.
16. AES – Advanced Encryption Standard, erstatter DES som symmetrisk blokkchifferstandard.
17. Vernamchiffer – også benevnt ’one-time pad’, kryptosystem basert på enkel XOR-operasjon av nøkkel og klartekst, er informasjonsteoretisk uknekkelig ved kjentchiffertekstangrep dersom nøkkelstreng er valgt uniformt tilfeldig og ikke gjenbrukes.
18. SHA – Secure Hash Algorithm FIPS PUB 180-1 1995
19. IPsec ESP – Encapsulation Security Payload spesifiserer subprotokoll for kryptering og autentisering av IP-pakker.
20. crypt(3) – enveisfunksjon for beskyttelse av passord i Unix/Linux operativsystem, algoritmen er avledet fra DES.
21. Se figur 2.2 i læreboka
22. Let the block be divided in a left half L and right half R, and the round key is K. $R_2 = L_1$ xor $F(R_1,K) = L_1$ xor $F(L_2,K)$ implies $L_1 = R_2$ xor $F(L_2,K)$. Hence a Feistel function is its own inverse (involution).
23. Se kap. 2.3 side 44 i læreboka.
24. En funksjon *f* fra argumentmengden *X* til billedmengden *Y* kalles en enveisfunksjon dersom det finnes en polynomisk tid algoritme som beregner

$f(x)$ for alle x i X, men samtidig der det for "essensielt alle" elementer y i Y ikke finnes noen polynomisk tid algoritme for å finne en x slik at $f(x) = y$. Med "essensielt alle" menes hele X muligens unntatt en delmengde med størrelse eksponensielt avtagende relativt til en økende størrelse på X (asymptotisk argument).

25. La g være generator av den multiplikative gruppen Z^*_p , hvor p er et stort primtall. La $x \in Z^*_p$. Da er $f(x) = g^x \bmod p$ en beregningsmessig enveisfunksjon.
26. Se figur 10.1 i læreboka.
27. Se slide 5 og 6 i forelesning 12.
28. Se side 330 i læreboka.
29. Når alle eksekverbare filer er "infisert" vil virusprogrammet henge i evig løkke i subrutinen infect_executable.
30. Dette blir en spesiell variant av "stoppeproblemet" (the halting problem). Det finnes veldefinerte beregningsproblemer som er "ubestemmelige" (undecidable). Antagelsen om at D finnes impliserer ved hjelp av konstruksjonen W en kontradiksjon. Den logiske konsekvens er at det ikke kan finnes ett generelt program eller sett av programmer som kan konsekvent bestemme er et software virus".
31. (a) 18^2 mod 3061 = 324
    (b) 18^4 mod 3061 = 324^2 mod 3061 = 902
    (c) 18^8 mod 3061 = 902^2 mod 3061 = 2439
    18^12 mod 3061 = ((18^8) * (18^4)) mod 3061 = (b)*(c) mod 3061 = 2180.
32. (a) 349^12 mod 3061 = 805, beregningsmetode for eksempel som ovenfor med tre kvadreringer og en multiplikasjon. Alternativt x^12 = (x^3)^4 .

    … kanskje du vil finne Alice sitt hemmelige tall $\log_{18 \bmod 3061}(349)$ også, 3061 er jo ikke et stort primtall sikkerhetsmessig…

-sfm 20050805.