

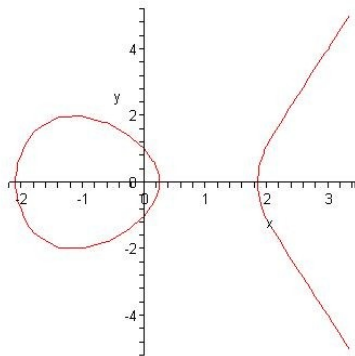
Proeftentamen: Security 2
Modulecode: INFSEC02
Docent: L.V. de Zeeuw
Datum: 2005/2006

- Dit tentamen bestaat uit 40 vierkeuze opgaven.
- Slechts één van de vier antwoorden is juist.
- Bij het tentamen mag **geen** gebruik worden gemaakt van rekenmachine, boeken, aantekeningen of andere bronnen van informatie.

1. Wat wordt bedoeld met klare tekst (plaintekst, cleartekst)?

- A. De originele begrijpelijke boodschap.
- B. De getransformeerde, onbegrijpelijke boodschap.
- C. Geclassificeerde tekst.
- D. Gedeclassificeerde tekst.

2. Dit is een voorbeeld van een:



- A. Elliptische kromme
- B. Ellips met hyperbool
- C. Ellips met parabool
- D. ECC

3. Beschouw de volgende uitspraken:

I Cryptografie staat in veel landen op dezelfde lijst als militaire wapens en munitie en mag niet worden geëxporteerd.

II Cryptografie mag overal in de wereld vrij gebruikt worden ter bescherming van je privacy.

Welke van deze uitspraken zijn waar?

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

4. Bij welk begrip is er geen rol voor cryptografie?

- A. Vertrouwelijkheid
- B. Authenticiteit
- C. Onweerlegbaarheid
- D. Beschikbaarheid

5. Modificatie is een aanval op:

- A. Beschikbaarheid
- B. Vertrouwelijkheid
- C. Integriteit
- D. Authenticiteit

6. Beschouw de volgende beweringen:

- I Bij reductieve maatregelen is er een rol voor encryptie.
- II Bij detectieve maatregelen is er een rol voor encryptie.

Welke beweringen zijn juist?

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

7. Beschouw de volgende beweringen:

- I Bij detectieve maatregelen is er een rol voor encryptie.
- II Bij correctieve maatregelen is er een rol voor encryptie.

Welke beweringen zijn juist?

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

8. Beschouw de volgende beweringen:

- Bij een substitutiecijfer ...
- I worden tekens vervangen.
 - II de volgorde van tekens gewijzigd.

Welke beweringen zijn juist?

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

9. Beschouw de volgende beweringen:

I De Caesar-cijfer is een voorbeeld van een mono-alfabetisch transpositiesysteem.

II De Vigenère-cijfer is een voorbeeld van een poly-alfabetisch transpositiesysteem.

Welke beweringen zijn juist?

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

10. Over hoeveel sleutels beschikt een gebruiker bij de symmetric-key cryptografie?

- A. 1
- B. 2
- C. 3
- D. 4

11. Hoeveel sleutels zijn er nodig in een symmetrisch cryptosysteem bij 10 deelnemers om elk paar personen met elkaar te laten communiceren zonder dat de anderen kennis kunnen nemen van de inhoud van de berichten?

- A. 45
- B. 55
- C. 90
- D. 110

12. DES is een afkorting van ...

- A. Data Encryption System
- B. Data Encryption Standard
- C. Data Emulation System
- D. Digital Encryption Standard

13. Hoeveel bits is de sleutellengte bij Triple DES?

- A. 56 bits
- B. 112 bits
- C. 128 bits
- D. variabel

14. Beschouw de volgende uitspraken:

I Een voordeel van Triple DES is dat deze lastiger te kraken is.

II Een voordeel van Triple DES is dat DES gebruik maakt van bestaande encryptie/decryptie hardware/software.

III Een voordeel van Triple DES is dat het gebruikt kan worden voor het zetten van digitale handtekeningen.

Welke van deze uitspraken is/zijn waar?

A. alleen I

B. alleen II

C. I en II

D. I, II en III

15. Beschouw de volgende uitspraken:

I een nadeel van Triple DES is dat er meer tijd nodig is voor encryptie/decryptie.

II een nadeel van Triple DES is dat het alleen gebruikt kan worden voor het zetten van digitale handtekeningen.

Welke van deze uitspraken is/zijn waar?

A. Beide zijn goed

B. I is goed en II is fout

C. I is fout en II is goed

D. Beide zijn fout

16. Onderstaande DES tabel is een:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

A. Initieële permutatie

B. Expansie box

C. Rotatie tabel

D. Permuted Choice

17. $DES(DES(M, K), K) = M$

Treedt op bij het gebruik van:

A. Sterke sleutels

B. Semi sterke sleutels

C. Semi zwakke sleutels

D. Zwakke sleutels

18. $DES(DES(M, K), K) = M$

Wat betekent dit?

A. Sterke encryptie omdat hier twee keer DES wordt gebruikt.

B. Twee maal vercijferen van message M met sleutel K

C. Twee maal vercijferen van message M met DES bij gebruik van sleutel K levert weer message M

D. Dit is onzin.

19. Hoeveel verschillende bewerkingen gebruikt DES?

- A. 1: Alleen Optelling modulo 2 (XOR)
- B. 2: Optelling modulo 2 (XOR) en optelling modulo 216
- C. 3: Optelling modulo 2 (XOR), optelling modulo 216 en vermenigvuldiging modulo 216
- D. 4: Optelling modulo 2 (XOR), optelling modulo 216 vermenigvuldiging modulo 216 en delen modulo 2

20. Hoeveel sleutelparen zijn er nodig in een asymmetrisch cryptosysteem bij 100 deelnemers om elk paar personen met elkaar te laten communiceren zonder dat de anderen kennis kunnen nemen van de inhoud van de berichten?

- A. 10
- B. 100
- C. 1000
- D. 10000

21. Wat zijn éénrichtingsfuncties?

- A. Functies die zelf gemakkelijk uit te rekenen zijn, maar het bepalen van de inverse is aanzienlijk moeilijker.
- B. Functies die zelf gemakkelijk uit te rekenen zijn, maar het bepalen van de inverse is aanzienlijk makkelijker.
- C. Functies die zelf moeilijk uit te rekenen zijn, maar het bepalen van de inverse is nog veel moeilijker.
- D. Functies die zelf moeilijk uit te rekenen zijn, maar het bepalen van de inverse is aanzienlijk makkelijker.

22. Beschouw de volgende uitspraken:

I Omdat hashfuncties sneller zijn dan handtekening functies is het efficiënter om een handtekening te berekenen van een hash van een bericht dan hiervoor het volledige bericht te gebruiken.

II Omdat hashfuncties sneller zijn dan handtekening functies is het efficiënter om een handtekening te berekenen van een hash van een sleutel van een bericht dan hiervoor het volledige bericht te gebruiken.

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

23. In een public-key cryptosysteem ontvangt B een digitaal gesigneerde boodschap van A. Met welke sleutel controleert B de digitale handtekening van A?

- A. de publieke sleutel van A
- B. de publieke sleutel van B
- C. de privé sleutel van A
- D. de privé sleutel van B

24. In een public-key cryptosysteem ontvangt B een gecijferde boodschap van A. Waarmee ontcijfert B het bericht van A?

- A. de publieke sleutel van A
- B. de publieke sleutel van B
- C. de privé sleutel van A
- D. de privé sleutel van B

25. Een bekend public-key cryptosysteem is het zogenaamde RSA-systeem. Waarvoor staat de afkorting RSA

- A. Remote System Access
- B. Ronald Shannon Adleman
- C. Redundant Security Check
- D. Rivest Shamir Adleman

26. Beschouw de volgende uitspraken:

- I RSA is een secret-key cryptosysteem.
- II RSA is een public-key cryptosysteem.
- III RSA is een symmetrisch cryptosysteem.
- IV RSA is een asymmetrisch cryptosysteem.

- A. I is goed en II is fout
- B. I is fout en II is goed
- C. I en II
- D. II en IV

27. Beschouw de volgende uitspraken:

- I Bij het RSA systeem moet de algoritme geheim blijven.
- II Bij het RSA systeem moet de encryptiesleutel geheim blijven.
- III Bij het RSA systeem moet de decryptiesleutel geheim blijven.

- A. alleen I
- B. alleen II
- C. alleen III
- D. geen van drieën

28. Voor een RSA sleutel generatie kiest Anna als priemgetallen $p=5$ en $q=7$. Voor de berekening van de privé sleutel heeft men een getal K nodig waarbij $K=(p-1)(q-1)$. Als getal e kiest Anna 11. Vervolgens wordt vastgesteld dat inderdaad geldt $1 < e < K$ én $\text{GGD}(e,K)=1$.

Om nu de privé-sleutel d te kunnen bepalen moet uitgerekend worden: $e \cdot d = 1 \pmod{K}$

Hoe groot is d ?

- A. 9
- B. 11
- C. 53
- D. 87

29. Als een superstijgende rij $a'=(1,3,5,10,22)$ en $S=14$ wat is dan de binaire vector x ?

- A. (1,1, 0,1,0)
- B. (1,3,10)
- C. (1x1,1x3,0x5,1x10,0x22)
- D. 0
0101010
0

30. Beschouw de volgende uitspraken:

I Sleutelgeneratie is een voorbeeld van activiteiten van sleutelmanagement
II Sleuteldistributie is een voorbeeld van activiteiten van sleutelmanagement

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

31. Beschouw de volgende uitspraken:

I Een sterke sleutel is een sleutel die moeilijk te raden is en gemakkelijk te onthouden.
II Een sterke sleutel is een sleutel die zorgt voor een moeilijk te kraken cijfertekst.

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

32. Beschouw de volgende uitspraken:

I Een certification Authority (CA) is onderdeel van een PKI
II Een Registration Authority (RA) is een onderdeel van een PKI

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

33. Wat is geen netwerkbeveiligingstechniek tegen indringers?

- A. encryptie
- B. firewall
- C. digitale handtekening
- D. locking

34. Beschouw de volgende uitspraken:

I Bij e-commerce gaan de gedachten uit naar nieuwe manieren om geld te verdienen door het verhandelen van elektronische producten.

II Met e-business wordt aan gegeven dat gebruik van internet geïntegreerd wordt in het gehele bedrijfsproces.

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

35. Beschouw de volgende uitspraken:

I Een nadeel van e-commerce is dat bedrijven veel extra kosten moeten maken om zich mondiaal te kunnen manifesteren

II Een voordeel van e-commerce is dat het producenten extra mogelijkheden biedt om informatie te krijgen over het koop gedrag van consumenten.

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

36. Beschouw de volgende uitspraken:

I Cryptografie is geen voorwaarde binnen e-commerce.

II Trusted Third-Parties vervullen geen belangrijke rol binnen e-commerce.

- A. Beide zijn goed
- B. I is goed en II is fout
- C. I is fout en II is goed
- D. Beide zijn fout

37. ${}^4\log 64 = ?$

- A. 2
- B. 3
- C. 4
- D. 5

38. $2^x = 8$.

$x = ?$

- A. 1
- B. 2
- C. 3
- D. 4

39. $\text{ggd}(242, 2442) = ?$

- A. 2
- B. 3
- C. 11
- D. 22

40. De inverse van 3 (mod 5) is ?

- A. 1
- B. 2
- C. 3
- D. 4

Aantal vragen per categorie:

Inleiding	4
Geschiedenis	1
Basisprincipes	3
Symmetric-key cryptografie	10
Public-key cryptografie	10
Sleutelbeheer	3
Toepassingen	4
Wiskunde	5
Totaal	40