Examination Secure Data Management

192110940 (UT students)

192110941 (Kerckhoff students)

- November 1st, 2013 -

Instruction:

- **This is an open book examination**
- **No electronic devices allowed**
- **The examination consists of TWENTY multiple-choice questions; each has the same weight: 5 POINTS**
- **Success!**

1/ Assume that all devices have the same probability of being revoked. Which device in the following media key block has the highest chance of getting blocked due to ***other*** devices being revoked?

WAL	GEP	ADE
CPL	CAP	WDC
DAL	BAC	GPE

A/ D
B/ G
C/ P
D/ W

2/ What is the Prime p of the Finite Ring $\mathbb{F}_p[x]/(x^{p-1}-1)$ used for searching in the following XML structure?

```
                   NodeA
                 /   |   \
          NodeB    LeafA    NodeC
           /  \              /  \
      NodeD   LeafB     LeafC   NodeE
       /  \                       |
  LeafD leafE                   LeafF
```

A/ p = 7
B/ p = 11
C/ p = 13
D/ p = 17

3/ Which version of OMA supports fully secure super distribution?

A/ OMA v1 Combined Delivery mode
B/ OMA v1 Separate Delivery mode
C/ OMA v2 Group Functionality
D/ None of the above

4/ What is the key difference between Copy Protection and DRM?

A/ Copy Protection rules Copy Control while DRM rules Usage Control
B/ Copy Protection is used for discs; DRM is used for Internet
C/ Copy Protection rules Copy Control while DRM rules Access Control
D/ There is no fundamental difference

5/ Assume attributes with corresponding terms A – t1, B - t2, C – t3, D – t4, E – t5 and F – t6. Which Subjects will get access under the policy encoded as c. = (τ, g^{12}, $m^*e(g,g,)^{12*\alpha}$ g^{5*t1},g^{3*t2},g^{3*t3},g^{2*t4},g^{2*t5},g^{5*t6}) ?

A/ Those that have at least attributes A, B and E
B/ Those that have at least attributes F, C, D and E
C/ Those that have at least attributes B, D and E
D/ Those that have at least attributes A and D

6/ Given the following SQL query "SELECT sub1, sub2 FROM tab1, tab2 WHERE sub1.att=sub2.att". Assume the following mapping functions.

tab1.att	tab2.att
[100 – 200) -> 1	[100 – 250) -> 9
[200 – 300) -> 3	[250 – 500] -> 6
[300 – 400) -> 8	
[400 – 500] -> 7	

What is the correct representation of the query condition on the encrypted tables?

A/ ((sub1)^S.att=1 AND (sub2)^S.att=9) OR ((sub1)^S.att=3 AND (sub2)^S.att=9) OR ((sub1)^S.att=8 AND (sub2)^S.att=6) OR ((sub1)^S.att=7 AND (sub2)^S.att=6)
B/(100 < (sub1)^S.att < 200 AND 100 < (sub2)^S.att < 250) OR (200 < (sub1)^S.att < 300 AND 100 < (sub2)^S.att < 250) OR (200 < (sub1)^S.att < 300 AND 250 < (sub2)^S.att < 500) OR (300 < (sub1)^S.att < 400 AND 250 < (sub2)^S.att < 500) OR (400 < (sub1)^S.att < 500 AND 250 < (sub2)^S.att < 500)
C/ ((sub1)^S.att=1 AND (sub2)^S.att=9) OR ((sub1)^S.att=3 AND (sub2)^S.att=9) OR ((sub1)^S.att=3 AND (sub2)^S.att=6) OR ((sub1)^S.att=8 AND (sub2)^S.att=6) OR ((sub1)^S.att=7 AND (sub2)^S.att=6)
D/ /(100 =< (sub1)^S.att < 200 AND 100 =< (sub2)^S.att < 250) OR (200 =< (sub1)^S.att < 300 AND 100 =< (sub2)^S.att < 250) OR (200 =< (sub1)^S.att < 300 AND 250 =< (sub2)^S.att < 500) OR (300 =< (sub1)^S.att < 400 AND 250 =< (sub2)^S.att =< 500) OR (400 =< (sub1)^S.att =< 500 AND 250 =< (sub2)^S.att =< 500)

7/ What is the effect of removing the random value r in the ABE access control term $d_0=g^{-r}$?

A/ Removing r will block access to attribute r
B/ Removing r allows users to collude
C/ Removing r will make the scheme more efficient
D/ Removing r reduces the number of policies that are supported

8/ Which role does the DDH assumption play in game based security analysis of the El Gamal scheme?

A/ It serves to prove that Pr[Attacker succeeds in game 1] - Pr[Attacker succeeds in game 2] is negligible
B/ It serves to prove that $\Pr[B(g^x, g^y, g^{xy}) = 1] = ½ + \varepsilon$
C/ It serves to prove that $|\Pr[B(g^{z1}, g^{z2}, g^{z1z2}) = 1] - \Pr[B(g^{z1}, g^{z2}, Z) = 1]|$ is negligible
D/ It serves to prove that $Enc_{mi} = (g^x, m_i g^{xy})$

9/ Which point below is **NOT** on the (3,6) Shamir Secret Sharing polynomial with secret 67 and random $a_1=3$ and $a_2=7$? ← fout

$a_1 = -7$ $a_2 = 3$

A/ (2, 65)
B/ (7,165)
C/ (6,131)
D/ (5, 107)

10/ In the wildcard search what will be the effect on the term below in case there are no wildcards in the query word?

$$\prod_{\substack{i=1 \\ i \notin J}}^{n} U_i^{w'_i \prod_{j \in J}(i-j)}$$

A/ The term will evaluate to 0
B/ The term will evaluate to 1
C/ The term cannot be evaluated
D/ The term will evaluate to a specific number representing the query word

11/ Delegated search: how will the Delegate step $t_*=(t_1, t_2, t_3, t_4)= (\gamma^a \cdot pk_S^{r1}, \gamma^{r1}, \gamma^{ya} \cdot pk_S^{r2}, \gamma^{r2})$ look like in case delegation is based on group G?

A/ $t_*=(t_1, t_2, t_3, t_4)= (\gamma^a \cdot pk_g^{r1}, \gamma^{r1}, \gamma^{ya} \cdot pk_g^{r2}, \gamma^{r2})$
B/ $t_*=(t_1, t_2, t_3, t_4)= (g^a \cdot pk_S^{r1}, g^{r1}, g^{ga} \cdot pk_S^{r2}, g^{r2})$
C/ $t_*=(t_1, t_2, t_3, t_4)= (\gamma^a \cdot pk_S^{g}, \gamma^{g}, \gamma^{ya} \cdot pk_S^{r2}, \gamma^{r2})$
D/ $t_*=(t_1, t_2, t_3, t_4)= (g^b \cdot pk_S^{r1}, g^{r1}, g^{gb} \cdot pk_S^{r2}, g^{r2})$

12/ Delegated search: which step in the scheme would not work properly in case the symmetry property of the bi-linear mapping does not hold?

A/ KeyGen
B/ Delegate
C/ TrapGen
D/ Test1

13/ Which of the following statements is **FALSE**?

A/ Bilinear maps exist on certain elliptic curves
B/ A commitment scheme cannot be both computationally hiding and computationally binding
C/ In an unconditionally binding commitment scheme, no computationally limited adversary can reveal two different values
D/ The shares in the Blackley secret sharing scheme are hyper planes

14/ What is the role of a ROM mark?

A/ A ROM mark prevents bit-wise copies because the different ROM mark of the destination disc prevents proper decryption
B/ A ROM mark prevents copying a disc bit-wise because the ROM mark blocks copying
C/ A ROM mark prevents bit-wise copies because the ROM mark of the original disc prevents any decryption
D/ A ROM mark prevents copying a disc bit-wise due to the missing ROM mark of the destination disc preventing encryption

15/ Which of the following functions over the natural numbers is a homomorphism from addition to multiplication?

A/ $f(x) = x^2$
B/ $f(x) = 2x$
C/ $f(x) = 2^x$
D/ $f(x) = x+2$

16/ Given a path p = $label_1/label_2/.../label_5$, and a function g(x) which turns a label into a natural number representing the binary representation of the first character of the label. Which hash function h(p) is expected to have least collisions?

A/ h(p) = $(f(label_1)*f(label_2)*...*f(label_5))$ MOD 13, where f(x) = 2*g(x)
B/ h(p) = $(f(label_1)*f(label_2)*...*f(label_5))$ MOD 11, where f(x) = g(x) MOD 2
C/ h(p) = $(f(label_1)*f(label_2)*...*f(label_5))$ MOD 11, where f(x) = $(g(x))^2$
D/ h(p) = $(f(label_1)*f(label_2)*...*f(label_5))$ MOD 13, where f(x) = g(x) MOD 2

17/ Which of the following statements is false?

A/ Mandatory Access Control (MAC) is used in most modern consumer operating systems.
B/ Role Based Access Control (RBAC) is particularly suitable for a company with a high turnover.
C/ In biometrics, false-positives are much worse than false-negatives.
D/ Biometric properties can change over time.

18/ Consider the Search in Encrypted Data approach from Song, Wagner, Perrig. Which statement below is **FALSE**?

A/ The search is linear.
B/ The approach exploits X xor K = C and C xor X = K.
C/ The approach exploits the homomorphic property of K.
D/The approach exploits X = X1 | X2 and X1 = F(X2).

19/ An RSA SecurID token is an example of an authentication method that is:

A/ Asynchronous.
B/ Based on a shared secret between the server and a token.
C/ Both A/ and B/.
D/ Neither A/ or B/.

20/ Which of the following sets forms a CYCLIC GROUP with the given algebraic operation?

A/ $Z^*{}_n$ with addition MOD n for n ∈ N

B/ $Z^*{}_{15}$ with multiplication MOD 15

C/ $Z^*{}_6$ with multiplication MOD 6

D/ Zp with multiplication MOD p for a prime p

Toets Parel 000 der Informatica (201300070)

6 september 2013, 10:45–11:45

- Je mag 1 zelfgemaakt A4'tje met aantekeningen bij dit tentamen gebruiken. Rekenmachines, laptops, mobiele telefoons e.d. zijn niet toegestaan. ***Stop deze nu in je tas!***
- Het aantal te behalen punten per opgave staat in de marge.

1. Binaire getallen

(a) Reken het 1-complements binaire getal 10101 om naar decimaal. Laat zien hoe je dit berekent. $\boxed{7}$

(b) Reken het hexadecimale getal A5 om naar decimaal. Laat zien hoe je dit berekent. $\boxed{7}$

(c) Stel je hebt een 8-bits unsigned binair getal en je schuift alle bits 1 plek naar rechts, en vult links een 0 aan. Met welke rekenkundige bewerking correspondeert dit, en waarom? $\boxed{7}$

(d) Verder over de vorige deelvraag: werkt dit ook goed als het 8-bits getal een signed 2-complements getal zou zijn? Waarom? $\boxed{4}$

2. Booleaanse logica

Iemand wil een schakeling bouwen die van twee input-bits A en B, naar keuze de OR of de AND berekent, onder besturing van een derde inputbit C; C=0 voor OR en C=1 voor AND.

(a) Geef de waarheidstabel hiervan. $\boxed{8}$

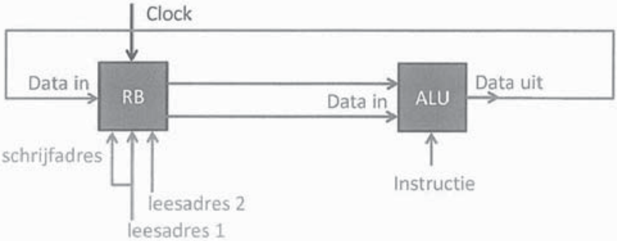
(b) Vereenvoudig de volgende Booleaanse formule en geef daarbij aan welke Booleaanse rekenregel(s) je gebruikt; begin met het wegwerken van het '+'-teken. $\boxed{9}$
$\mathsf{A} + \overline{\mathsf{A} \cdot \mathsf{B}}$

(c) Schets hoe je met alleen NOR-poorten de volgende formule kunt realiseren: $\boxed{8}$
$\mathsf{A} + \overline{\mathsf{B} + \overline{\mathsf{C}}}$

Zie volgende bladzijde...

3. Opgave 3

20



Bovenstaande simpele processor kent twee instructies: 0 = '+' (optellen) en 1 = '*' (vermenigvuldigen).

Geef voor deze processor het programma voor de volgende bewerking: R2 = (R1+R2)*(R0+R1)

	leesadres 1 / schrijfadres	leesadres 2	instructie
Tijdslot 0			
Tijdslot 1			
Tijdslot 2			
Tijdslot 3			
Tijdslot 4			
...			

4. Opgave 4

30

Gegeven het volgende AVR-programma ("BRNE" betekent "BRanch if Not Equal", "MUL" betekent MULtiply, "DEC" betekent "DECrement (verminderen met 1)" en "SUB" betekent "Subtract"):

```
LDI R16, $03
LDI R17, $03
LDI R18, $02
LDI R20, $01
MUL R17, R18
DEC R16
MOV R19, R16
SUB R19, R20
BRNE -5
```

Geef in tabelvorm aan hoe de inhoud van de registers verandert terwijl dit programma doorlopen wordt; dat mag hexadecimaal of decimaal, naar keuze, maar laat wel zien wat je kiest.

Einde van deze toets.