**MT Exam CMPE-552 26.11.2019 (60 min, 30 points)**

St. Name, Surname\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ St.Id#\_\_\_\_\_\_\_\_\_\_\_\_\_

**Closed book, electronic devices are not allowed**

Instructor Alexander Chefranov

**Totally 3 questions, 5 pages**

Good Luck!

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Question | 1 | 2 | 3 | Total |
| Point | 10 | 10 | 10 | 30 |
| Grade |  |  |  |  |

**Task 1. (10 points)** What is an access control list? What is a capability list? What is the difference between them? Give examples.

Access control list (ACL) is a list of subjects related to a resource where for each subject, allowed accessing the resource, allowed operations on the resource are specified.

Capability list (CL) is a list related to a subject where for each resource, the subject is allowed accessing, allowed operations are specified.

Difference is that access control lists are arranged for resources and show what subjects (people, processes) and how can access them, whereas capability lists are arranged for subjects and show what resources and how can be used by them.

Examples:

ACL: File1=>u1|R,w=>u2|r

CL: U1=>File1|R,w=>File2|w

**Task 2. (10 points)** For a multiplicative cipher, encrypt and decrypt back the first two letters of the following text: “Security” using the key, k=7. Give necessary explanations.

Hints:

$$c\_{i}=k∙p\_{i} mod 26$$

$$p\_{i}=k^{-1}∙c\_{i} mod 26$$

EXTENDED EUCLID(m,b)

1. (A1,A2,A3):=(1,0,m); (B1,B2,B3):=(0,1,b);
2. if B3=0 return A3=gcd(m,b); no inverse
3. if B3=1 return B3 = gcd(m,b); B2= b-1 mod m
4. Q=
5. (T1,T2,T3):=(A1-QB1, A2-QB2, A3-QB3)
6. (A1,A2,A3):= (B1,B2,B3)
7. (B1,B2,B3):= (T1,T2,T3)
8. goto 2

Code table:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Code | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| Letter | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |

P=“SE” => (18, 4)

Encryption: $c1=k∙p1 mod 26=7∙18=126 mod 26=22=W$

$$c2=k∙p2 mod 26=7∙4=28 mod 26=2=C$$

Thus, ciphertext is “WC”

Decryption needs $k^{-1}mod 26$. Find it using Extended Euclid algorithm:

1. A=(1,0, 26), B=(0,1,7)

$$q=\left⌊A3/B3\right⌋=\left⌊26/7\right⌋=3$$

T=A-qB=(1,-3,5)

1. A=(0,1,7), B=(1,-3,5)

$$q=\left⌊A3/B3\right⌋=\left⌊7/5\right⌋=1$$

T=A-qB=(-1,4,2)

1. A=(1,-3,5), B=(-1,4,2)

$$q=\left⌊\frac{A3}{B3}\right⌋=\left⌊\frac{5}{2}\right⌋=2$$

T=A-qB=(3,-11,1)

1. A=(-1,4,2), B=(3,-11,1)

B3=1 => B2= $7^{-1}mod 26=-11 mod 26=15$

Check it: $7∙15 mod 26=105 mod 26=\left(4∙26+1\right) mod 26=1$

Decryption: $P1=c1∙15 mod 26=22∙15 mod 26=330 mod 26=\left(12∙26+18\right)mod 26=18=p1='S'$

$$P2=c2∙15 mod 26=2∙15 mod 26=30 mod 26=\left(26+4\right)mod 26=4=p1='E'$$

Thus, restored plaintext is “SE” as expected.

**Task 3. (10 points)**

1. Draw E-R diagram for a database keeping records on teachers being academic advisors of students with two entities and one relation. Specify primary key and two more attributes of entities in the E-R diagram.

Advises

Teacher

Student

Primary keys are underlined.

1. Specify schemes of tables for the entities and relation.

|  |
| --- |
| Teacher |
| TID | Name | Surname |

|  |
| --- |
| Student |
| StID | Name | Surname |

|  |
| --- |
| Advises |
| TID (FK) | StID (FK) |

1. What are the primary key attributes of the relation table? What foreign keys are used in the relation table?

PK is (TID, StID), The both attributes are foreign keys referencing Teacher (TID), and Student (StID).

1. What is the mapping cardinality type of the relation (1-1, 1-m, m-1, m-m)? Why?

Mapping cardinality is 1-m, with Teacher being side 1, and Student being side m. Teacher is side 1 because, for any one student there shall be at most one teacher. Student is side m because any one teacher may have many (more than one) advised by him/her students.

1. Give an example of violation data consistency for the database under consideration

Database will be inconsistent if, e.g., one student has two advisors.