Report No. 4

Information Security October 21, 2020 Group: 23

Antonin Thioux (s3791378) & Xiaoyu Guan (s3542807)

1.

Solution:

8. CRC-Checksum(10101011) = 1010
   Other examples are CRC-Checksum(0110) = 1010 and CRC-Checksum(10101) = 1010
9. Trudy could use the following data values in the form 111xxxxx; 11100011, 11110000.

2. See code on Themis.
3. See code on Themis.
4.

Solution:
The number of possibilities for GPG keys $= 2^{(16\times4\times10)} = X$.
This means the probability of a non match is $1 - \frac{1}{X} = p$.
Give the probability of n non matches $p(n)$ the probability of n+1 non matches is $p(n+1) \approx p(n) \times p^n$.
With the base case of $p(2) = p$.
This gives us $p(n) \approx \prod_{i=1}^{n-1} p^i \approx p^{\sum_{i=1}^{n-1} i} \approx p^{\frac{(n-1)n}{2}}$
For $p(7.5 \cdot 10^9) \approx p^{\sum_{i=1}^{(7.5\cdot10^9)-1} i}$
We take the 'worst case' $p(7.5 \cdot 10^9) \geq 1 - \frac{2^{70}}{X} \approx 1 - \frac{2^{70}}{2^{640}} = 1 - 2^{-570}$.
This means the probability of two or more people sharing the same finger print is $1 - (1 - 2^{-570}) = 2^{-570} \approx 0$.

5.

Solution:

1. conflict classes:

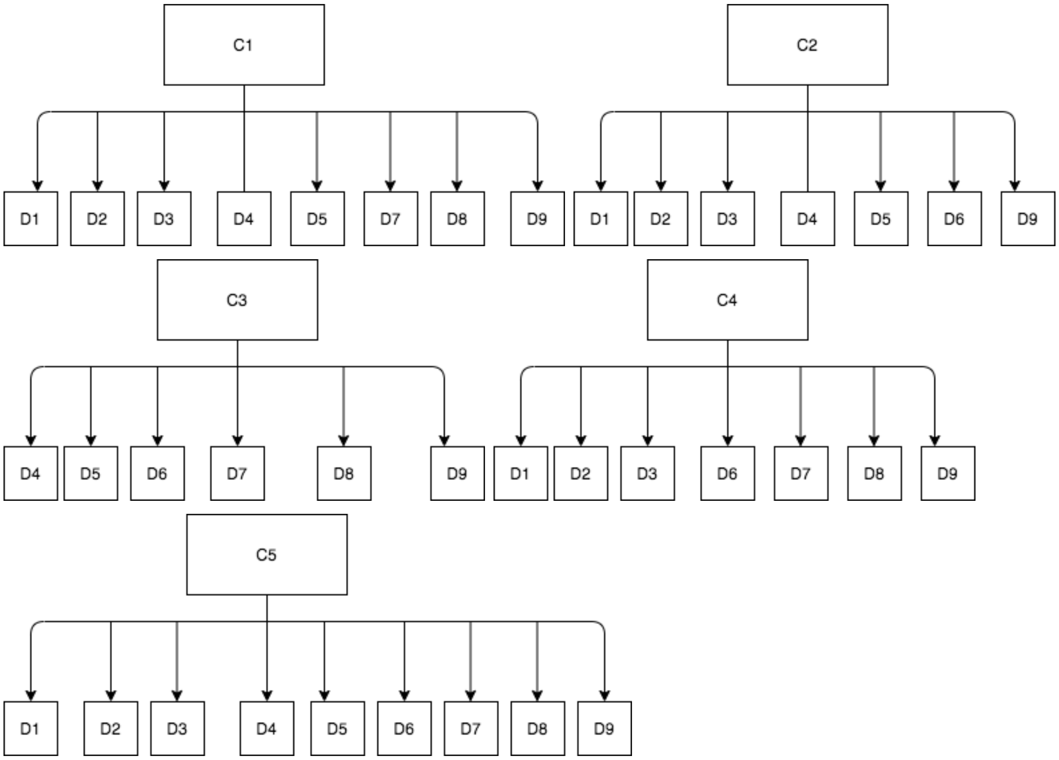
   $\{C_1, C_3\}$

   $\{C_2, C_4\}$

   $\{C_5\}$

   According to the definition of the Chinese Wall policy, it is used to control the data accessed by other who have interest conflict and also since both C_1 and C_3 are from oil industry they might have possibility conflict of interests they are put in same conflict class, for the same reason C_2 and C_4 are from finance industry they will be in the same conflict class. Finally, only C_5 is from insurance industry there is only one object in this class.

2. A company can access other documents that are not in the same conflict class



6.

Solution:

1. In the first $< Target >$ block's first $< Anyof >$ is used to check if the subject of request is from "Manger". And the second one is used to determine whether the report is "Report1"

   The second $< Target >$ is used to check if the the first $< Anyof >$ request is from "Client" and the second one is to determine if the confidential is true.

2. The request will be denied because will the role is "Manager" which gives access to "Report1" they are not a client hence they do not have access to "confidential", because this policy uses the deny override algorithm the denied access to "confidential" will deny access of the entire request.

7.

Solution:

1. The lifetime of tickets are required(e.g TGT, ST), which can be used to ensure that the ticket is valid otherwise it will not be passed the authentication process. This means the ticket can only be used within the time frame and the client can't hold on to it for future communication.

2. Message H contains $the\_time\_auth + 1$ encrypted with service session key such that the client can decrypt it and verify that it is indeed communicating with someone that can decrypt the cipher message and not an imposter pretending to be the Service Server. Since the Service Server is the only one who can read the decrypt the cipher message once the client receives message H he/she knows they are communicating with the Service Server.

8.

Solution:

1. According to the textbook
   (a) Client indicates the thought of connecting with server and along with the cipher list and nonce R_A
   (b) Server makes certification and choose one of the cipher text that sent by client and along with nonce R_B to client
   (c) Client generates a random pre-master secret and a key that used to encrypted the message that checked by hashing function(this hashing can check if the previous messages are sent correctly)
   (d) Client authenticates Server if hashing function matched
   (e) The key is shared between Client and Server
2. It means Client can trust the Server and can make sure Client will send message to a right server that also help Client to keep his/her information's safe.
3. So that the client can make sure that they are downloading code from a trusted website and the code they downloaded is safe to run.

   CA organization: TERENA

   CA final: DIGICERT
4. FROM Wednesday, 14 February 2018 at 1:00:00 AM Central European Standard Time TO Thursday, 18 February 2021 at 1:00:00 PM Central European Standard Time

9.

Solution:

1. k-anonymity level is $k = 2$

   Explanation: Each quasi-identifiers tuple appears in at least k records, which in this case to find the minimum number of tuples is 2 $(Caucasian, 21)$.

2. Yes, there is problem

   Since this table contains Homogeneity data (e.g all (Afro-American,34) has Flu, (Caucasian, 21) has Viral and (Hispanic, 18) has Cancer), once attacker knows that person's race or age attacker can know the disease.

   L-Diversity requires at least l distinct values in each equivalence, which avoid the problem that all the people from a same tuple have same disease.

   Solution with L-diversity: $l = 2$

Race	**Age**	**Disease**
Afro-American	34	Flu
Caucasian	21	Viral
Caucasian	21	Flu
Hispanic	18	Cancer
Afro-American	34	Cancer
Hispanic	18	Viral
Afro-American	34	Viral
Hispanic	18	Flu

10.

Solution:

1. Problem: With the increase of using data for statistics or other study purpose should not increase the risk of personal privacy violation.

   Work: Adding noise into data.

2. $b = \epsilon = 2$

   $\mu = max|Q(1) - Q(2)| = 30$

   noise $= 2 * (\mu/\epsilon)^2 = 450$

   $K(Q(1)) = 450 + 10 = 460$

   $K(Q(2)) = 450 + 40 = 490$