1) Question

a. The confidentiality is about keeping the data from getting it into the hands of unauthorized access.It is mostly to protect people’s privacy for example in a hospital the patient’s data is crucial because if the data goes or falls into the wrong authorities then they going to use it for their motives which is dangerous so that’s why confidentiality is important while handling data.

Integrity is about keeping the credibility, accuracy, and Trustworthiness of data is very important because the data that is acquired from unauthorized access would have less trust data than authorized access. For instance, online the OTPs that come through the authorized bank have more trust than an OTP from an unauthorized place.

Availability is about having service to the data, emergency response, telecommunications and as other services that need a connection. So, availability of the data is crucial in many services for example in emergency responses need to have a connection that is always available for emergencies.

b. Confidentiality vs. Availability: If confidentiality is increased then the availability of the data going to be reduced as the confidentiality is about encrypting the data. Once the data is encrypted the availability for the data to use would reduce it for example when the availability is reduced due to confidentiality it gets hard to get data from the database and always need to get permission in reducing the availability when the confidentiality is higher.

Integrity vs. Confidentiality:If data integrity checks, such as cryptographic hashing, are implemented to bolster data integrity, it may necessitate the inclusion of additional metadata or checksums alongside the data. Although this enhances integrity, it could inadvertently compromise confidentiality by potentially leaking information about the data. For instance, the presence of checksums in encrypted files could offer attackers insights into the content of the data.

Availability vs. Integrity: If redundancy and failover mechanisms are implemented to improve availability, it could introduce potential vulnerabilities that attackers could exploit to compromise data integrity. For instance, maintaining multiple copies of data across geographically distributed servers for high availability raises the risk of data inconsistency or divergence if synchronization mechanisms fail.

2) Question

KITLKE.

Answer:

1. The plaintext is that “thrill” has the key values as

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| T - 111 | H - 001 | R - 101 | I - 010 | L - 100 | L - 100 |
| K - 011 | I - 010 | T - 111 | L - 100 | K - 011 | E - 000 |
| L - 100 | K - 011 | I - 101 | S - 110 | T - 111 | L - 100 |

The plaintext for thrill = LKISTL this is the key.

1. The plaintext is that “tiller” has the key values as

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| T - 111 | I - 010 | L - 100 | L - 100 | E - 000 | R - 101 |
| K - 011 | I - 010 | T - 111 | L - 100 | K - 011 | E - 000 |
| L - 100 | E - 000 | K - 011 | E - 000 | K - 011 | R - 101 |

The plaintext for tiller = LEKEKR this is the key. These are the values of the keys based on the above tables.

3)Question

3)a. Answer: The total keys of the 40-bit key would be 240 then the average of this would be ½ of 240 which would make the calculations like:( ½ \* 240 = 239). So, Trudy tries before she finds the correct one is 239.

3)b. Trudy will know when she has found the correct key by decrypting the ciphertext using each possible key and examining the resulting plaintext. However, since there are too many possible keys to manually examine each one, Trudy needs an automated approach to determine whether a putative key is correct or not by knowing the similarities in the cipher text and plain text by looking into their language similarities as if they could know once the language resembles any known language such as English. If Trudy can guess some part of the text, then turdy can verify it with the output text and find out if the deciphered text is correct or wrong or if she could. Find out about the context of the code then the deciphered text has the same meaning then turdy can confirm the text. By checking as, I have stated turdy can verify the legitimacy of the text.

3)c. The work that the automated test in part b would completely be dependent on the complexity of the text and the characteristics, as well as the length of the text, would all make the work required for the text deciperation but we can calculate some of the time that other parts of the brute force attack require that could be the number of keys that are the 40-bit key which would give 240 types of deciphering. It may take a long as turdy need to use every key to check with all the given cipher keys also checking the keys would take up a lot of time as well as checking if the deciphered text is correct or not would also take up time. This all would make the time taken to increase comparatively.

3)d. When a false key yields a putative decryption that passes the test, false alarms can happen, giving Trudy the false impression that she has located the correct key because then we can’t guess the complexity of the cipher text, and as we don’t know the cipher text complexity we going to face a lot of false alarms when we try to know if the text is correct or wrong compare to a simple test. The quality of the text will make multiple false alarms as the correct or incorrectness of the text going to be difficult to find the plain text, The test sensitivity is also one of the factors in causing false alarms if the test sensitivity is high, it causes a lot more of false alarms comparatively with low test sensitivity.

4)a. The size of the keyspaces would be 628 because there are 8-character mixed-case alphanumeric keys and the keys used in it are 0-9, a-z, and A-Z which would be a total of 62 characteres by using this all we get the size of the keyspaces as 628.

b. By following the hint: rewrite the size of the keyspace as a power of two then it would make the equation as follows:

2x  = 628

Log 2x = log 628

x = 8log 262

x = 8 \* 5.9542 (as we know the value of log 262)

So, x = 47.6336 bits. (Which we can take round value of x that leads to 48 bits)

c. If a particular computer can test 240 keys per second, Then the time taken to guess the cipher text would be as

follows:

we get the values from part b such as x values then by using that we solve the equation to get.

x =

Then the x value would be 28 seconds.

Then by doing average we get ½\*28 = 27

27 = 128

Hence the total time taken for the computer to average time taken = 128 seconds.

5)a. The new size of the keyspace = 264

b. The time that would it take to crack the new version of the cipher if able to test 240 keys per

second then

x =

x = 224 bits per seconds

Hence, The time taken would be a total of 224  bits per second (that would be 194 days approximately).