Cryptography and Network Security-Report Submission

The name and photo associated with your Google account will be recorded when you upload files and submit this form. Not **snehlata1503@gmail.com**? Switch account

* Required

Email address *

va6573@bennett.edu.in

Name *

Vidisha Arvind

Roll Number *

E18CSE209

Email ID *

VA6573@bennett.edu.in

Name of the team members with roll numbers: *

Kinshuk Gupta (E18CSE088)
Himanshu Mittal(E18CSE063)

Project Title *

QuantCertificate: Quantum Cryptography based Digital Signature for verifying certificate

Describe your project (Your answer will be more than 200 words-2 Marks)

We are building a website that uses the notion of qubits in quantum key exchange over the quantum channel to secure candidate certificates provided by a specific institution. It effectively utilizes the quantum digital signature technique in which symmetric key cryptography is used. Random basis for each bit of the message will be selected on the sender's side, which is private to the sender and will be encoded using basis and sent then each qubit will be randomly calculated at the receiver's end, which will be private to the receiver. Now, both sender and receiver will publicly share basis that they used for every qubit if receiver measured the qubit in a similar basis which sender prepared it in, then it will be uses to form part of their shared secret key, otherwise message shared will be discard for that particular bit.Lastly, secret key is used for both sender and the receiver in order to encrypt and decry-pt information which will be hashed in form of image of 256 bits using wavelet transformation at the sender's end and AES(Advanced encryption standards) is implemented on hashed message and the secret key for encryption of the information and then that encrypted message is stored in the database and to view message at receiver’s again AES is applied on the message received.

Motivation and contributions of the project (Clearly specify the problem statement and contributions-2 Marks)

Quantum computing is the future of computing and its arrival, though very limited has already made cryptographic algorithms which were once considered unbreakable, obsolete. Considering this we realized that there is a need for more innovative methods that can be used to keep our data secure in the age of Quantum computers.
So, we decided to develop a simple web app to demonstrate Quantum Cryptography. Through our web app a user can send a file to another user through quantum encryption. This ensures that the data transmission is secure and even warns the user when its message is intercepted by an unwanted third party. We have used Quantum Key Distribution along with AES encryption to protect the file transfer.

How it will be different from similar existing solutions (Your answer will be more than 200 words-2 marks)

To our knowledge, there is no publicly available application or code which uses quantum key distribution for creating shared key to use symmetric encryption methods like AES, and Triple-DES, therefore this makes our project unique. There are lot of noticeable differences:
- We use quantum key distribution to generate shared key which promises that there is no way of intercepting communication and even try to read message as qubits change their state upon measuring with different basis than the sender, hence any such action can be easily caught
- This allows secure communication between two party without even sending the shared key. It solves the problem that secure key is not possible without secure channel, and secure channel is not possible without secure key, but our solution solves this problem as it can generate secure key in any channel and allow creation of secure channel, completely eliminating any potential loopholes.
- We use AES-256 using the generated shared key for encryption/decryption process to make it more robust and solid (as AES-256 is considered the de-facto algorithm by today's standards).
- For creating message digest when message is in the form of images, we use modified wavelet transform, an image hash function for creating 256-bit hash to be sent in symmetric encryption methods.
We have demonstrated this using a simple web app, with clean interface. The code is available publicly.

Design diagrams related to your project (Block diagram/architectural diagram/activity diagram/data flow diagram. At least one diagram, you suppose to draw and upload. Kindly, use some tools for drawing the figures-2 marks [Note: Do not draw using pen and paper]) *

FLOWCHART OF ... BLOCK DIAGRA...

Add file

Implementation and Results (Give the implementation details and upload screenshots related to the results [Upload the separate PDF file]-2 Marks)

Screenshots and...

One Impressive Post on LinkedIn regarding your Project (At least 100 words and one Image and 5 hashtags, Tag at least CSE Bennett handle-3 marks [Note: Every team member should post on LinkedIn, Give the URL links here])

1] https://www.linkedin.com/posts/activity-6736698405369741312-ZY6D/
2] https://www.linkedin.com/posts/himanshumittal13_quantumtechnology-cryptography-cybersecurity-activity-6736688865588867072-_Uxu
3]https://www.linkedin.com/posts/kinshuk-gupta_quantumtechnology-cryptography-cybersecurity-activity-6736697354218467328-05X2

Implementation (Project code)/ Draft Code (Give Link of Github or any other public Repository/ Web Link where your partial code is available to see-2 Marks)

https://github.com/Kinshukg04/Crypto_project

Submit