**Data Security and Cryptology – Project Report**

* Project Topic:

An application for secure SMS exchange: encryption-decryption with Kuznyechik in CBC mode, including DH key generation and signature EC ElGamal

* Components:

1. Kuznyechik is a symmetric block cipher. It has a block size of 128 bits and key length of 256 bits.
2. Cipher block chaining (CBC) is a mode of operation for a block cipher.
3. The ElGamal signature scheme is a digital signature scheme based on the algebraic properties of modular exponentiation, together with the discrete logarithm problem.
4. ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields

* Key Exchange:

For resolving key exchange in the symmetric algorithm, we use Diffie Hellman which is a mathematical method of digital encryption that securely exchanges cryptographic keys between two parties over a public channel without their conversation being transmitted over the internet. To make sure that no one is tampering with algorithm Alice and Bob attach digital signature using EC ElGamal to their public keys so the other part can verify that they got the right key

* ENCRYPTION :

Check KEY – Must be 256-bit

Text –partition the text to 128-bit each block,

If the last block is less than 128-bit, then add ‘1’ and then pad with zeroes to all the bits to be 128-bit.

In CBC mode loop on the blocks as hex and encrypt each block using Kuznyechik

Concatenation all ciphertext to one string and return it

* DECRYPTION:

Check KEY – Must be 256-bit

Text –partition the text to 128bit each block

Decrypt according to Kuznyechik and CBC mode

* Digital signature:

Alice generates digital signature on her message using EC ElGamal, and Bob verifies the signature after decryption to make sure that he got the right message

* The Project Flow:

Alice wants to send a secure SMS to Bob.   
Alice and Bob use Diffie Hellman exchange keys to compute shared key:

Alice and Bob agree on (p,g) values

Alice and Bob choose their private keys

Alice and Bob compute their public key

Alice and Bob generate a signature for their public keys using EC ElGamal

Alice and Bob share with each other their public keys and its digital signature

Alice and Bob verify each other digital signature using EC ElGamal

Alice and Bob compute their shared key

Alice writes a message

Alice generates a digital signature on her message using EC ElGamal

Alice generates initial vector (IV) for CBC

Alice encrypts the message using Kuznyechik in CBC mode

Alice shares the ciphertext, IV, digital signature with BOB

Bob receives them from Alice

Bob decrypts the ciphertext using Kuznyechik in CBC mode

Bob verifies the digital signature

* Conclusions:

The algorithm implemented employs a robust combination of cryptographic techniques to ensure secure communication and data protection.

Kuznyechik encryption algorithm in CBC mode offers strong confidentiality by encrypting data blocks with a secret key.

Diffie Hellman key exchange, used for secret key delivery, provides secure key exchange through public channel. Additionally, EC ElGamal signature scheme adds an extra layer of authentication and integrity verification, ensuring the legitimacy of the sender.

Together, these techniques provide a comprehensive approach to encryption, decryption, and secure key delivery, bolstering the overall security of the system.