LOCATION BASED ELLIPTIC CURVE CRYPTOGRAPHY

BY:-

ANUP KUMAR PANIGRAHY(82)

CHODEN LAMA(67)

GROUP-32

MENTOR:-

UTPAL KUMAR RAY

What is ECC?

- Elliptical curve cryptography (ECC) is a public key encryption technique based on *elliptic curve theory* that can be used to create faster, smaller, and more efficient cryptographic keys.
- ECC generates keys through the properties of the elliptic curve equation.
- The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman.
- ECC is more secured because it requires less bits space compared to other techniques like RSA.

ENCRYPTION

- Alice selects a point P on the curve, as his plaintext message P(done by message passing algorithm).
- He then calculates a pair of points on the curve as cipher-texts:

  $C_1 = r * e_1$

  $C_2 = p + r * e_2 + L_k * e_1$, where r is a random integer
- Alice sends these two cipher-texts , C_1 and C_2 to Bob.

DECRYPTION

- Bob, after receiving C_1 and C_2, calculates plain-text message ,P using the following formula:-

  $P = C_2 – (d * C_1) – (L_k * e_1)$

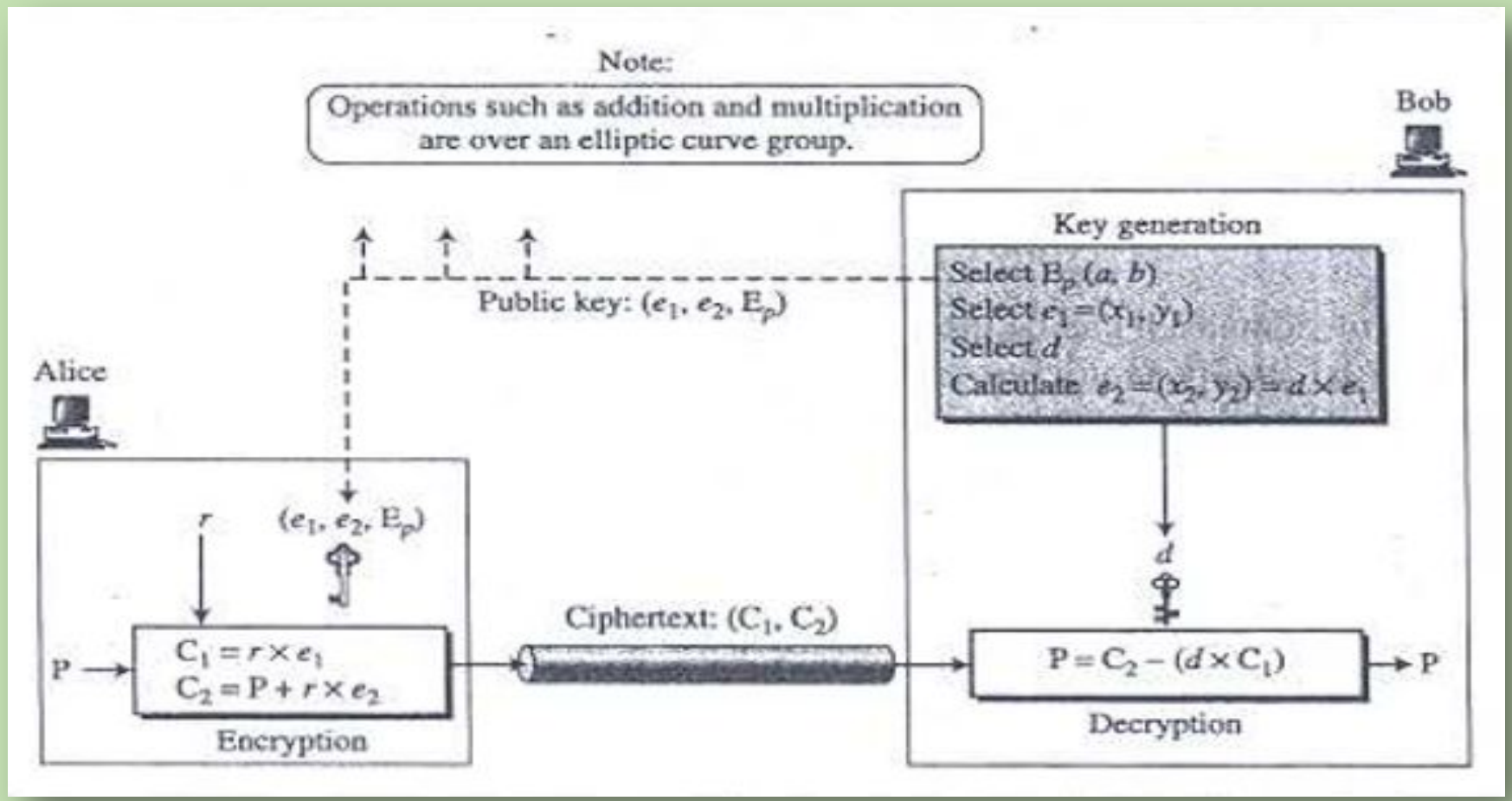
  The minus sign here means adding with the inverse.

- This P obtained is a point on the elliptic curve, which is converted into plain-text message using reverse-mapping algorithm.

COMPONENTS OF ECC

- Public Key :- A Random Number
- Private Key :- Point on a curve = Private key * G
- Set of operations :- These are defined over the curve $y^2 = x^3+ax+b$
- Domain Parameters :- G, a, b

How the ECC works?

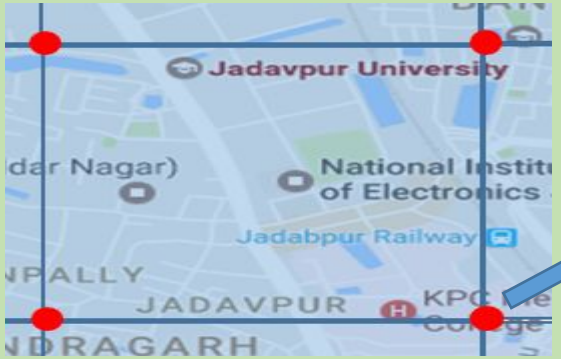


LOCATION KEY

- For implementation of Location based ECC, it is required to form a location key, which is another point on the elliptic curve.
- This location key is formed by the concatenation of location base point and time key and multiplying this concatenated value with the generator point on the elliptic curve.

LOCATION BASED POINT

- The map is divided into different grids of equal dimensions. Each grid has a base point marked with red dot. B.P. is located at the left-bottom corner of each grid.
- If the latitude is 22.789 and longitude is 44.126, then the coordinates are concatenated to form Location B.P. as Location BP = 2278944126.



B.P. of JU Campus

TIME KEY

- Time key varies with time, that is-

  if a person is present in that time frame then only he/she can decrypt that message.

- For example, JU Main Campus is open from 09:00:00 to 18:00:00 everyday. So, if sender sends message on 22/03/2018 to the receiver, then the receiver will be able to decrypt that message only if he is physically located inside the campus and receives the message before 18:00:00 on that particular date.
- For each date, 09:00:00 is considered as the B.P. of time frame. In this case, the time key used by the sender is concatenation of date and B.P. of that particular frame given by 12012018100000.

LOCATION KEY FORMATION

- Location key is formed using location B.P. and time key.
- Location Key = f(Location BP, Time Key)

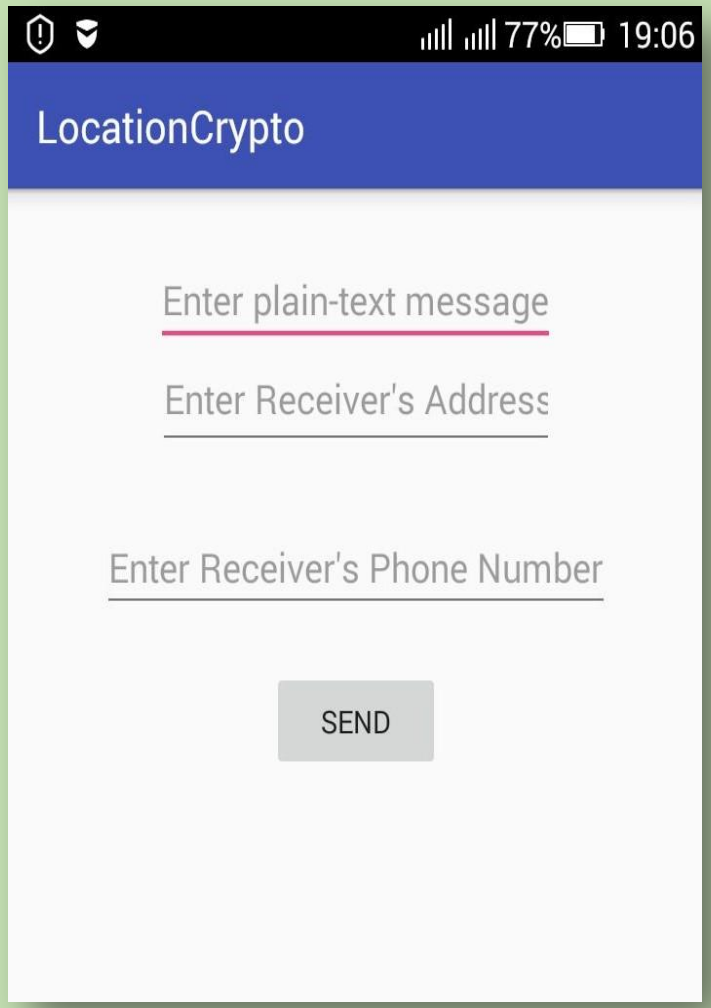
Here f() is considered as concatenation operation then Location Key is given by:

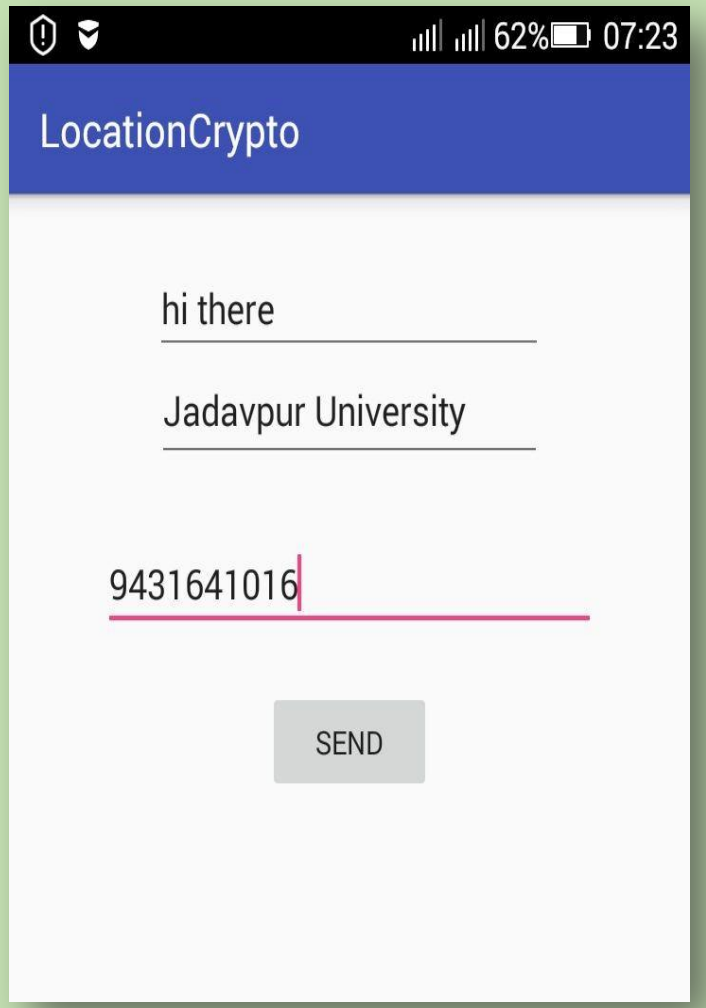
L_k = 2278944126 || 120120181000000

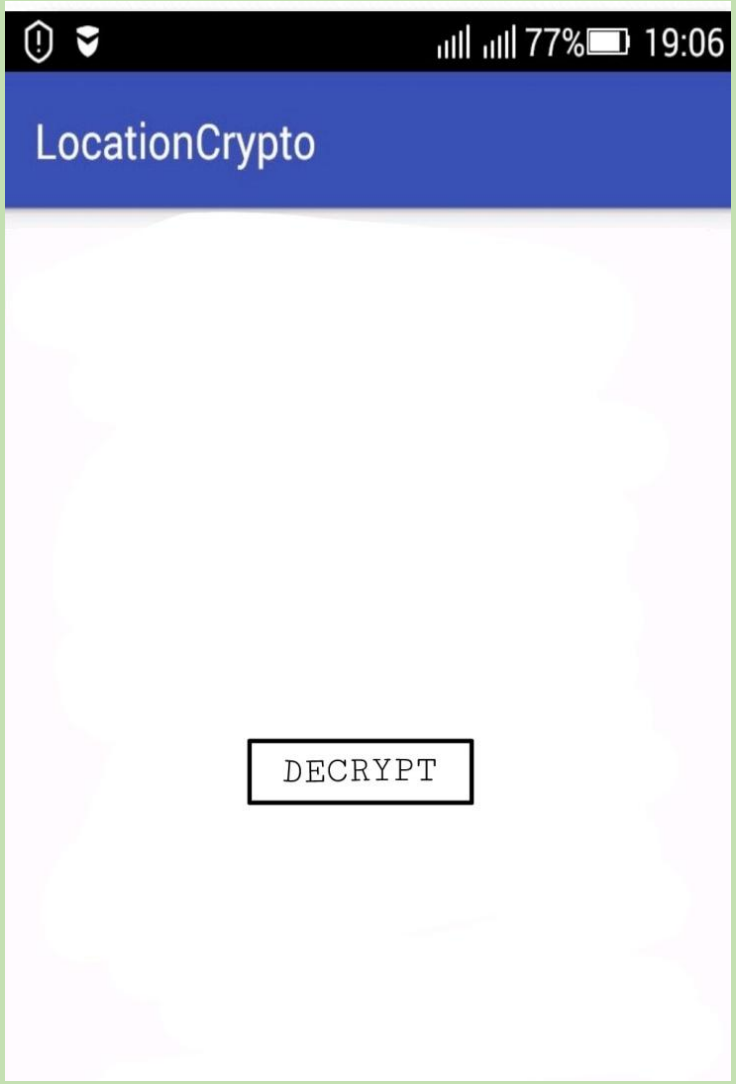
i.e. L_k = 227894412612012018100000.

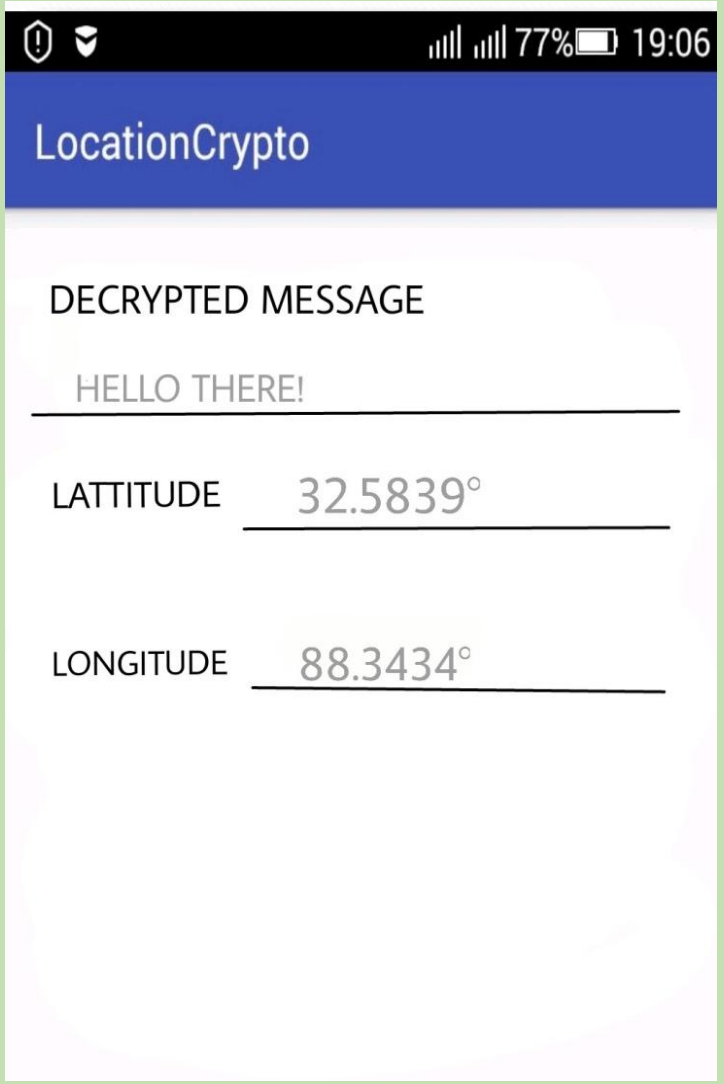
IMPLEMENTATION

RESULTS


77% 19:06
LocationCrypto
Enter plain-text message
Enter Receiver's Address
Enter Receiver's Phone Number
SEND


62% 07:23
LocationCrypto
hi there
Jadavpur University
9431641016
SEND


77%
19:06
LocationCrypto
DECRYPT


77%
19:06
LocationCrypto
DECRYPTED MESSAGE
HELLO THERE!
LATTITUDE
32.5839°
LONGITUDE
88.3434°

Location Detection of the receiver

SENDER'S END:

- The sender has to physically enter address at which the receiver is currently residing.
- The android.location.Geocoder classes of java is used and its method getFromLocationName(address, n) is called to get a list of all the n addresses close enough to this entered address.
- The methods getLatitude() and getLongitude() of Address class are used to get location coordinates of the receiver.

Location Detection of the receiver(Continued….)

RECEIVER'S END:

- The android.location.LocationManager class of java is used and its method getLastKnownLocation(LocationManager.GPS_PROVIDER) is called to get Location object.It means that this will access the GPS of receiver's mobile to get his location.
- The methods getLatitude() and getLongitude() of the Location class are used to get current location coordinates of the receiver.

Time key generation

- The java.util.Calendar class is used and its method getTime() is called to return a date object (of java.util.Date class).
- This date object is formatted using format(date) method of SimpleDateFormat class to bring it in the form “yyyyMMddHHmmss” .

Message Sending

- After encrypting plain-text message, the sender has to then send the generated cipher-texts to the receiver.
- The android.telephone.SmsManager class of java is used and its method sendMultipartTextMessage(phoneNumber,SMSC address,text-message,pending-intent(SMS sent),pending-intent(SMS delivered)) is used to send cipher-text to the receiver.

Message Receiving

- BroadcastReceiver class is created to listen for any incoming message at the receiver’s end.
- After that the phone number of the sender and the text message is fetched. This is done using methods like getOriginatingAddress() and getMessageBody() of SmsMessage class.
- The cipher text fetched is decrypted to obtain plain-text message, if possible.

ECC SECURITY

- To decrypt the message, Eve needs to find the value of r or d.
- If Eve knows r, he can use $P = C_2 – (r * e_2)$ to find the point P related to the plain-text. But to find r, Eve need to solve the equation $C_1 = r * e_1$. This means, given two points on the curve,C_1 and e_1, Eve must find the multiplier that creates C_1 starting from e_1. This is referred to as the ‘elliptic logarithm problem’ and the only method available to solve it is the ‘Pollard rho Algorithm’, which is infeasible if r and p have large values.

ECC SECURITY

- If Eve knows d, he can use $P = C_2 – (d * C_1)$ to find the point P related to the plain-text. Because $e_2 = d * e_1$, this is the same type of problem.
- Hence, the security of ECC depends solely on the difficulty of solving the ‘elliptic curve logarithmic problem’.

REFRENCES

- Cryptography & Network Security – Behrouz A. Forouzan.
- Lecture Notes and other materials provided by our Mentor Prof. Utpal Kumar Ray.
- ECC information from Wikipedia

  https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

THANK YOU