**DIGITAL SIGNATURE IN BLOCKCHAIN:**

**ECDSA**

This algorithm is used in bitcoin and ethrium. It is an public key encryption algorithm which solves a group of an elliptic curve points. First of all the encryption is done on the basic property of the elliptical curve that it is symmetric along x axis ,the curve used for bitcoin and ethrium is called sect256k1 which in a form of equation is y^2=x^3+7. It has a property that any two point on the curve added together will give third point on the curve and then the symmetric point can also be plotted(symmetric along x-axis). Suppose we have a point p then we can calculate the third point using p+p and so on . The algorithm is used for 256 bit integer so there will be maximum of 510 steps to get the result let x be the integer then total no of combination of the integer will be 2^255 we need to compute xp which will give a result let it be X then we can give the equation as X=xp here we cannot get x using X which satisfies the property of public key encryption and so X can be taken as public key and x be the private key. This also has an advantage that there is no complex computation of dIvision ,it can be easily computed just using addition

**Disadvantage:**

 A chance of error makes it possible to select a private key value such that identical signatures for different documents can be obtained. However, enormous computational performance is required for this chance to materialize.

**EGIAMAL ENCRYPTION SYSTEM**

It uses deffie Hellman encryption. It is an asymmetric encryption also ie. different key is used for encryption and decryption suppose there are two user A and B then A forms a mix of its private key and public key (Apub+Apri) and B forms a mix of its private key and public key (Bpri+Bpub)

Then these two exchange their mixture of the keys after the exchange of mixture the two add their private key to the exchanged mixture to obtain a secret key. This type of algorithm ensures encryption as well as digital signature.

This solution is employed in public key certificates for the purposes of protecting connections in TLS (SSL, HTTPS, WEB), messages in XML Signature (XML Encryption), and the integrity of IP addresses and domain names (DNSSEC).

**Disadvantage:**

The encrypted text length is doubled compared to the initial length this causes longer computation time and tougher requirements for communication channel.

**RABIN CRYPTOSYSTEM**

This algorithm is an extension of a rsa algorithm which can be solved using chinese remainder theorem. In this algorithm first two prime no is then such that both no on division with 4 gives a reminder as 3. Encryption is done as c=m^2modN, therefore there is 4 possible output on decryption which is given as mp=+-c^((p+1)/n)modp and mq=+-c^((q+1)/n)modq which can be solved using chinese remainder theorem and we have to select any one of the 4 outputs.

It has a higher operating speed vs RSA

**Disadvantage:**

It is needed to select necessary message out of the 4 possible outcome.

**IDENTITY BASED DIGITAL SIGNATURE**

In this algorithm the digital signature is been added based on the unique id of the receiver suppose there are different blocks in a block chain each have its unique id, as we are dealing with a private block chain the unique id of every block is known ,if a sender wants to send the data so that only a authorise person is able to access a data , the sender encrypts the data with the unique id of the receiver ,when the receiver decrypts the data it initially compare the id with the unique id of the receiver then only grants the permission to the receiver to view the data ie. if the receiver is not authorise then it will not be able to view the data even if the data is been received .The implementation of this also is very simple and works very well for a private blockchain

**CONCLUSION**

Comparing all the different algorithms such as RSA,ECDSA,EGIAMAL,RABIN CRYPTOSYSTEM,IDENTITY BASED DIGITAL SIGNATURE we came to conclude that identity based digital signature would be the better algorithm to be implemented as it does not need much high computation power and is better suited for the private blockchain authorisation.

**REFERENCES**

**1.**[**https://youtu.be/muIv8I6v1aE**](https://youtu.be/muIv8I6v1aE)

**2.**[**https://youtu.be/iwCYey4im6Y**](https://youtu.be/iwCYey4im6Y)

**3.https://youtu.be/mdxlFwRF4ek**