

I.서론

1,연구의 필요성 또는 동기

현재 **RSA**암호화 알고리즘이 대표적으로 사용되고있다. 하지만 **RSA**알고리즘보다 **ECC** 알고리즘이 좀 더 장점이 많다.예를들어 저장의 효율성, 대역폭의 절감등이 있다.우리는 **ECC** 알고리즘을 좀 더 보완하여 **RSA** 알고리즘을 대체하여 보다 더 보편화 시키기 위해 이러한 주제를 골랐다

2.연구문제

ECC 알고리즘과 **RSA** 알고리즘은 어떤 차이점이 있으며, **ECC** 알고리즘의 어떤 점을 보완해야 좀 더 보편화 될수 있을것인가? 또한 **ECC**알고리즘이 **RSA** 알고리즘에 비해 가지고있는 단점들은 무엇이있는가