# 공개키 알고리즘

# 대칭키 알고리즘

# 공개 키 암호

‘암호화 키’는 암호화를 위해 송신자가 사용하는 것

‘복호화 키’는 복호화를 위해 수신자가 사용하는 것

# 공개키와 개인키

\*\*도청자에게 알려지면 곤란한 것 : 복호화 키 (암호화키는 도청자에게 알려져도 괜찮음)

# 공개 키 암호의 종류

1. RSA
2. ElGamal(엘가말)

* 타헤르 엘가말이 1985년 고안한, 디피–헬먼 키 교환을 바탕으로 한 공개 키 암호 방식
* **이산 대수 문제의 어려움에 기반**을 둔 최초의 공개 키 암호 알고리즘.
* **Elgamal로 암호화하면 메시지의 길이가 2배로 늘어나는 특징이 있음. 암호화할 때 난수 k를 이용하므로 같은 메시지에 대해 암호화하여도 암호화할 때마다 서로 다른 암호문을 얻게 됨**. -> 정보보호 측면에서 큰 장점
* RSA에서는 난수를 사용하지 않아 같은 메시지에 대한 암호문은 항상 같다는 특징이 있음. 이것은 공격자가 암호문을 복호화하지 않고도 평문을 추측할 수 있는 단점이 되므로, 실제 적용 시 RSA는 난수를 사용하는 OAEP(Optimal Asymmetric Encryption Padding)이라는 난수화 패딩 알고리즘과 함께 사용
* 알고리즘 1) 키생성 – 큰 소수 p와 생성자 g를 선택, 개인키 x를 선택하고, 공개키 y=g^e mod p 계산 2) 암호화 – 평문 m을 암호화하기 위해 난수 k 선택, 암호문 a = g^k mod p, 암호문 b = my^k mod p, 암호문 [a,b]를 수신자에게 전달 3) 복호화 – 평문 m=b/a^x mod p로 계산

1. ECC(Elliptic Curve Crypto system, 타원 곡선 암호 시스템)

* 1985년 Miller와 Koblitz가 독립적으로 제안
* 타원곡선상에서 이산대수의 어려움을 기반으로 한 공개키 암호 알고리즘
* **기존 공개 키 암호화(RSA)보다 짧은 키의 길이로 동일한 안전성을 제공 (RSA 1024 bit = ECC 160 bit)**
* 하드웨어 및 소프트웨어 상에서 빠른 암/복호화 제공
* 초기 공개 키 암호 방식은 아주 큰 정수를 2개 이상의 소수로 나누는 것이 오래 걸리는 것에 기반을 두고 있음. 타원곡선 암호 또한 알려진 특정한 점에 대한 무작위 타원 곡선의 아신 로그를 찾는 것이 오래 걸린다는 것에서 착안,
* **암호화 목적으로 타원곡선은 평면곡선의 한 종류로 다음의 방정식을 만족하는 점(**[**무한 원점**](https://ko.wikipedia.org/wiki/%EB%AC%B4%ED%95%9C_%EC%9B%90%EC%A0%90)**포함)들의 집합이다. (곡선의 단순함을 위해 점들은**[**표수**](https://ko.wikipedia.org/wiki/%ED%99%98%EC%9D%98_%ED%91%9C%EC%88%98)**가 2나 3이 아닌 고정된**[**유한체**](https://ko.wikipedia.org/wiki/%EC%9C%A0%ED%95%9C%EC%B2%B4)**이다.)**
* **{\displaystyle y^{2}=x^{3}+ax+b}**
* **위 집합은 타원곡선의**[**군**](https://ko.wikipedia.org/wiki/%EA%B5%B0_(%EC%88%98%ED%95%99))**의 연산과 함께**[**무한 원점**](https://ko.wikipedia.org/wiki/%EB%AC%B4%ED%95%9C_%EC%9B%90%EC%A0%90)**을 항등원으로 하는**[**아벨 군**](https://ko.wikipedia.org/wiki/%EC%95%84%EB%B2%A8_%EA%B5%B0)**을 형성한다.**[**군**](https://ko.wikipedia.org/wiki/%EA%B5%B0_(%EC%88%98%ED%95%99))**의 구조는**[**대수다양체**](https://ko.wikipedia.org/wiki/%EB%8C%80%EC%88%98%EB%8B%A4%EC%96%91%EC%B2%B4)**를 밑으로 하는**[**인자**](https://ko.wikipedia.org/wiki/%EC%9D%B8%EC%9E%90_(%EB%8C%80%EC%88%98%EA%B8%B0%ED%95%98%ED%95%99))**를 따른다.**
* 무선 환경과 같이 전송량과 계산량이 상대적으로 열약한 환경에 적합
* 이론적으로 복잡하여 실제 구현에 어려움이 있음, 전원의 양의 한정된 이동 통신 기기의 암호화에 적용할 수 있어 차세대 공개 키 암호 방법으로 주목 받고 있음

1. 전자 서명(Digital Signature) <승철 tv 확인, 전공책 확인>

A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender ([authentication](https://en.wikipedia.org/wiki/Authentication)), that the sender cannot deny having sent the message ([non-repudiation](https://en.wikipedia.org/wiki/Non-repudiation)), and that the message was not altered in transit ([integrity](https://en.wikipedia.org/wiki/Data_integrity))

An **electronic signature**, or e-signature, refers to [data](https://en.wikipedia.org/wiki/Data) in electronic form, which is logically associated with other data in electronic form and which is used by the [signatory](https://en.wikipedia.org/wiki/Signature) to sign.[[1]](https://en.wikipedia.org/wiki/Electronic_signature#cite_note-Cryptomathic_WHATISADIGITALSIGNATURE-1)[[2]](https://en.wikipedia.org/wiki/Electronic_signature#cite_note-eIDAS_Reference-2)[[3]](https://en.wikipedia.org/wiki/Electronic_signature#cite_note-3) This type of signature provides the same legal standing as a handwritten signature as long as it adheres to the requirements of the specific regulation it was created under (e.g., [eIDAS](https://en.wikipedia.org/wiki/EIDAS" \o "EIDAS) in the [European Union](https://en.wikipedia.org/wiki/European_Union), [NIST-DSS](https://en.wikipedia.org/wiki/Digital_Signature_Standard) in the [USA](https://en.wikipedia.org/wiki/United_States) or [ZertES](https://en.wikipedia.org/wiki/ZertES" \o "ZertES) in [Switzerland](https://en.wikipedia.org/wiki/Switzerland)).[[4]](https://en.wikipedia.org/wiki/Electronic_signature#cite_note-Cryptomathic_MajorStandardsDigSig-4)[[5]](https://en.wikipedia.org/wiki/Electronic_signature#cite_note-5)

Electronic signatures are a legal concept distinct from [digital signatures](https://en.wikipedia.org/wiki/Digital_signature), a cryptographic mechanism often used to implement electronic signatures. While an electronic signature can be as simple as a name entered in an electronic document, [digital signatures](https://en.wikipedia.org/wiki/Digital_signature) are increasingly used in [e-commerce](https://en.wikipedia.org/wiki/E-commerce) and in regulatory filings to implement electronic signatures in a [cryptographically protected](https://en.wikipedia.org/wiki/Cryptography) way. Standardization agencies like [NIST](https://en.wikipedia.org/wiki/NIST) or [ETSI](https://en.wikipedia.org/wiki/ETSI) provide standards for their implementation (e.g., [NIST-DSS](https://en.wikipedia.org/wiki/Digital_Signature_Algorithm), [XAdES](https://en.wikipedia.org/wiki/XAdES" \o "XAdES) or [PAdES](https://en.wikipedia.org/wiki/PAdES" \o "PAdES)).[[4]](https://en.wikipedia.org/wiki/Electronic_signature#cite_note-Cryptomathic_MajorStandardsDigSig-4)[[6]](https://en.wikipedia.org/wiki/Electronic_signature#cite_note-CryptomathicDigSigServicesAshiqJA-6) The concept itself is not new, with common law jurisdictions having recognized [telegraph](https://en.wikipedia.org/wiki/Telegraph) signatures as far back as the mid-19th century and faxed signatures since the 1980s.

1. Rabin

* RSA 알고리즘의 변형, 미하엘 라빈이 1979년 1월에 발표한 소인수 분해 기반 공개키 암호(비대칭암호)이다. 공개키로 암호화하고, 개인키로 복호화한다. 중국인의 나머지 정리 (Chinese Remainder Theorem, CRT)를 활용
* RSA는 e,d라는 지수를 사용하지만, Rabin은 e,d가 2로 고정되어 있어 RSA보다 암호화 연산이 빠름
* 특징 1) 효율성(efficiency) : 암호화에서 square modulo를 계산하기 때문에 3차 이상 계산하는 RSA에 비해 효율적, 복호화에서 two modular exponentiations와 CRT를 적용하므로 RSA와 비슷 2) 효과성(effectiveness) : 암호화 함수가 4 to 1이므로, 복호화 과정에서 4가지 서로 다른 결과가 나오고 이중 3가지는 가짜 결과이므로, 푸는 과정에서 진짜 결과를 잘 추론 해야 함. 숫자 값을 암호화한 경우 모호성 제거 스킴 disambiguation scheme)를 사용해야 한다. 이 단점을 개량해 암호문1 : 평문 1을 유지하는 알고리즘이 쓰인다.

3) 보안성 (security) : 소인수 분해 문제와 동치. 동치성이 증명되거나 소인수분해 일반 공식이 등장할 때까지 훨씬 안전하고, 선택 암호문 공격(chosen ciphertext attack)에 취약할 수 있음

<https://ko.wikipedia.org/wiki/%EB%9D%BC%EB%B9%88_%EC%95%94%ED%98%B8%EC%B2%B4%EA%B3%84>

1. ECDSA(Elliptic Curve Digital Signature Algorithm)

: 타원 곡선을 이용한 DSA(디지털 서명 알고리즘)의 변형

https://en.wikipedia.org/wiki/Elliptic\_Curve\_Digital\_Signature\_Algorithm