$e \cdot d \equiv 1 \mod \phi(n)$

$e \quad d$

RSA Digital Signature: Security

$\phi(n) = (p-1)\cdot(q-1)$

- **Necessary hardness assumptions:**
  - **Factoring hardness assumption:** Given *n* large, it is hard to find primes pq = n
  - **Discrete logarithm hardness assumption:** Given *n* large, *hash*, and *hash*^{d} *mod n*, it is hard to find *d* → private key

$H(m)$

signature

$[H(m)]^d$

- Salt also adds security
  - Even the same message and private key will get different signatures

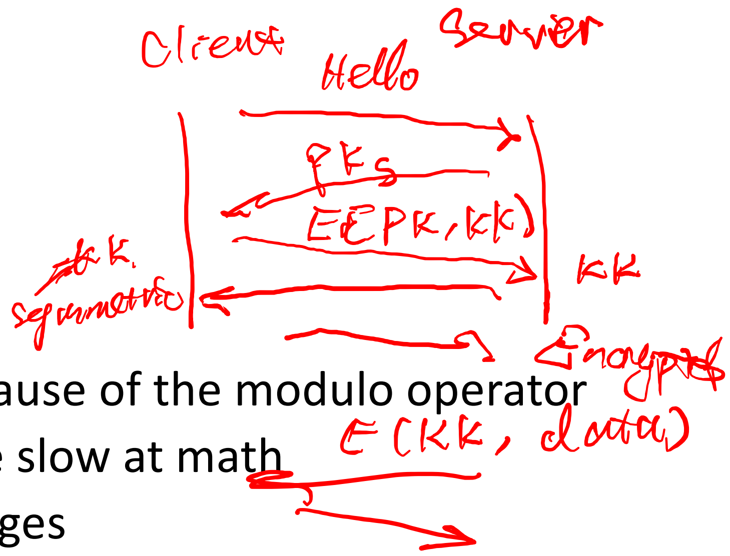
$y = H(m)^d$

$\text{dlog } y = \text{dlog } H(m)^d$

$= d[\text{dlog } H(m)]$

$\Rightarrow d = \dfrac{\text{dlog } y}{\text{dlog } H(m)}$

Hybrid Encryption



- Issues with public-key encryption
  - Notice: We can only encrypt small messages because of the modulo operator
  - Notice: There is a lot of math, and computers are slow at math
  - Result: We don't use asymmetric for large messages
- **Hybrid encryption**: Encrypt data under a randomly generated key *K* using symmetric encryption, and encrypt *K* using asymmetric encryption

  ↓ symmetric

  - Enc$_{Asym}$(PK, K); Enc$_{Sym}$(K, large message)
  - Benefit: Now we can encrypt large amounts of data quickly using symmetric encryption, and we still have the security of asymmetric encryption

TLS

Network Security

- Key Distribution and User Authentication

Chapter 4

Remote User Authentication Principles

4.1

Remote User Authentication Principles

- RFC 4949 defines user authentication as: “The process of verifying an identity claimed by or for a system entity.” This process consists of two steps:
  - Identification step: presenting an identifier to the security system
  - Verification step: presenting or generating authentication information that corroborates the binding between the entity and the identifier
- Fundamental security building block
  - Basis of access control & user accountability

Means of User Authentication

- Something the individual knows
  - password, PIN, answers to prearranged questions
- Something the individual possesses
  - token: cryptographic keys, electronic keycards, smart cards, and physical keys
- Something the individual is (static biometrics)
  - fingerprint, retina, and face
- Something the individual does (dynamic biometrics)
  - voice pattern, handwriting characteristics, and typing rhythm

News about Bitcoins

- In October 2025, the U.S. District Court for the Eastern District of New York disclosed an unprecedented case of cryptocurrency asset seizure: the U.S. government confiscated 127,271 bitcoins, worth about $15 billions at market price.
- **Root Cause: Weak Randomness in Key Generation:** It argues the underlying vulnerability is not a broken algorithm per se, but the use of a **non-cryptographically secure PRNG** during wallet/private-key generation. In particular, many “weak wallets” used the MT19937 (Mersenne Twister) generator with low entropy seeds, making private keys predictable.
- Lesson: Ensuring Cryptographic Randomness (i.e. not use system time as seed). Randomness and Private Key Security is the Lifeline of the Blockchain World

Solution?

When Randomness Isn't So Random: The Truth Behind the Theft of 120,000 BTC, https://www.bitget.com/amp/news/detail/12560605022352