cryptography

ROADMAP :D

Introduction

- Cryptography: 1 thuật ngữ trong tiếng anh mang nghĩa mật mã học
- Crypto (Krypto – greek): hidden, secret
- Graphien(Greek) : to write

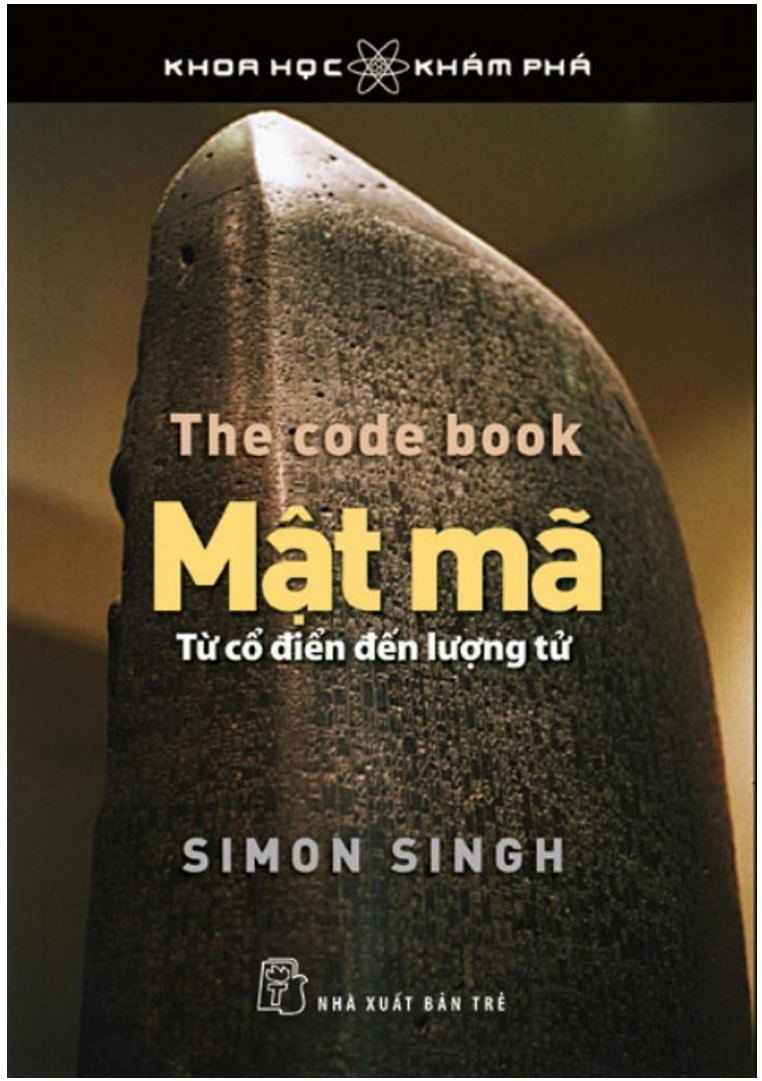
$\Rightarrow$ Cryptography : văn bản bị ẩn giấu

- Cryptography là 1 ngành khoa học nghiên cứu về mã hóa và giải mã thông tin, chuyển đổi thông tin từ dạng đọc hiểu được sang dạng mà con người không hiểu được (đọc nhưng không hiểu được thông tin) và ngược lại.

Introduction

- Cryptography đã có lịch sử từ rất lâu, lần đầu tiên được phát hiện vào khoảng 1900 TCN
- Mật mã học có tuổi đời lâu, tuy nhiên tầm quan trọng và sự phát triển của mật mã bắt đầu rõ rệt hơn là vào thời điểm CTTG II (thời điểm enigma ra đời và cũng là sự tiến hóa của kĩ thuật phá mã khi có sự tham gia của toán học)

Introduction



importance of cryptography

- Privacy and confidentiality: cryptography có vai trò bảo vệ, giữ thông tin an toàn, không lọt vào tay người khác, đảm bảo privacy và confidentiality
- Integrity: Đảm bảo tính toàn vẹn của dữ liệu
- Availability: đảm bảo rằng dữ liệu luôn có thể được access bất cứ thời điểm nào
- Authentication: xác thực, định danh người dùng, từ đó cung cấp quyền hạn tới những thông tin cần thiết.

what to learn

Number theory(introduction level)

- Euclidean algorithm, extend Euclidean
- Modular arithmetic
- Prime number
- Fermat little theorem
- Euler totient function/ euler theorem
- Testing primability – miller rabin algorithm
- Chinese remainder theorem
- Discrete logarithm
- Birthday attack, birthday paradox

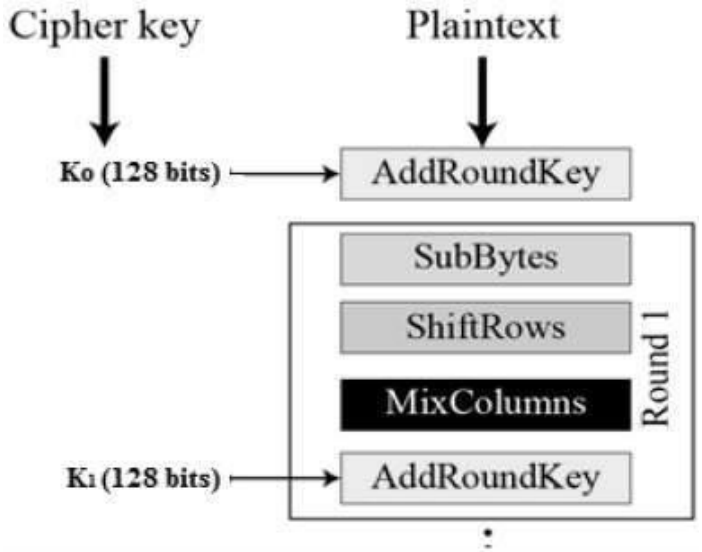
Number theory (advanced):

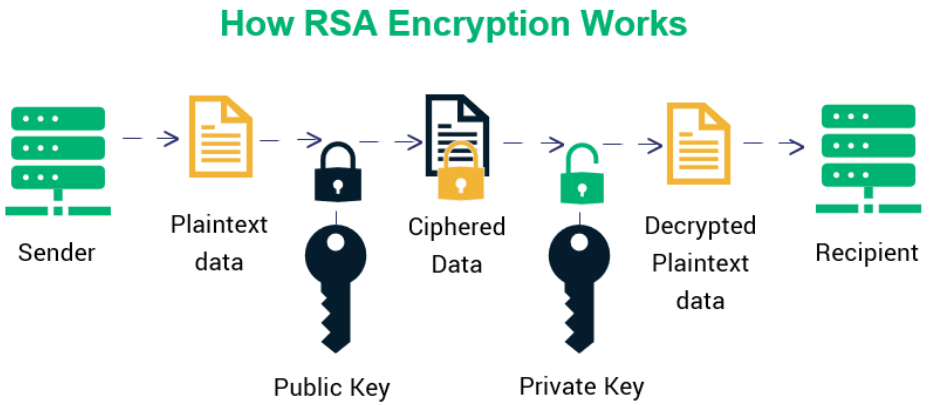
- Group/Ring/Field
- Finite Field of form GF(p), GF(p^k)
- Polynomial Arithmetic
- Linear algebra
- Lattice
- … (actually, you need to learn all)

what to learn

Symmetric cipher:

- AES
- DES (outdated)
- Stream cipher (rc4, salsa20, …)
- …





Asymmetric cipher:

- RSA (currently safe, but not in the future)
- Elliptic curve cryptography
- Diffie Hellman Key exchange
- Post-quantum
- Digital signature algorithm
- …

what to learn

- Hash function
  LCG
  RNG
  LSFR
  ...

Linear congruential method: D. H. Lehmer

◦ To produce a sequence of integers $X_1, X_2, \ldots$ between 0 and m-1 by following a recursive relationship:

$$X_{i+1} = (aX_i + c) \bmod m, \quad i = 0,1,2,\ldots$$

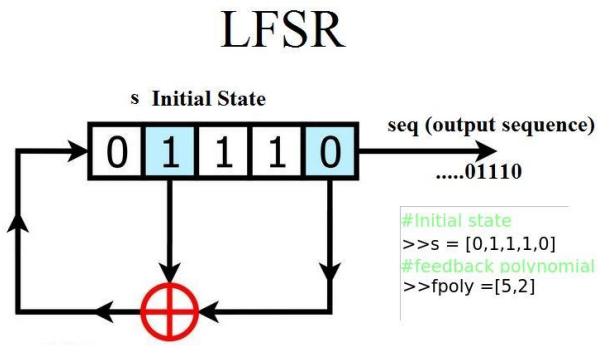
The multiplier | The increment | The modulus

◦ Assumption: $m > 0$ and $a < m$, $c < m$, $X_0 < m$

• The selection of the values for a, c, m, and X_0 drastically affects the statistical properties and the cycle length

• The random integers X_i are being generated in $[0, m\text{-}1]$

Let us choose $m = 2^{13}$, $a = 21$, $c = 5$



tools

- Python (highly recommend)
- Z3 library
- Sagemath
- WSL/ Vmware/ Virtual Box
- Vscode (of course you can do it on notepad, IF YOU CAN)
- Library that support cryptographic function (pycryptodome, , primefac, …)
- Online tools : (factordb, alpertron, hashkiller, …)

Practice

- cryptohack.org
- ctf.hackme.quest
- cryptopals.com
- Dreamhack.io
- Hack the box
- ctftime.org
- …

SLIDE

END :3