Cryptography Roadmap

Symmetric Ciphers
- Classical Ciphers
- Block Cipher & DES
- AES (ECB, CBC, CTR)

Asymmetric Ciphers
- RSA
- Diffie-Hellman KE
- ElGamal Cryptosystem
- Elliptic Curve ECC

Hash Functions
- SHA1 & SHA3
- MACS & HMAC
- Digital Signatures
- ElGamal DS scheme

Linear Algebra
- Linear Equations
- Matrices
- Vector Spaces
- Abstract Algebra
- Rings & Finite Fields

Number Theory
- Divisibility & GCD
- Factorization
- Prime Numbers
- Congruences & CRT
- Quadratic Residues
- Cubic and Elliptic Curves

Advanced

Internet Security
- X.509 Certificates
- SSL/TLS & HTTPS
- Secure Shell SSH
- Mail Security & PGP

Post-Quantum Crypto
- Code-Based
- Lattice-Based
- Multivariate
- Hash-Based

Linear Algebra
- Eigenvalues & Eigenvectors
- Inner Product Spaces
- Complex Vector Spaces
- Abstract Algebra

Number Fields
- Elliptic Curves over Finite Fields
- Structure of $U(Z/nz)$
- Primitive Roots
- Irreducible Polynomials
- Field Extensions
- Quadratic & Cyclotomic Fields
- Ideals & Lattices
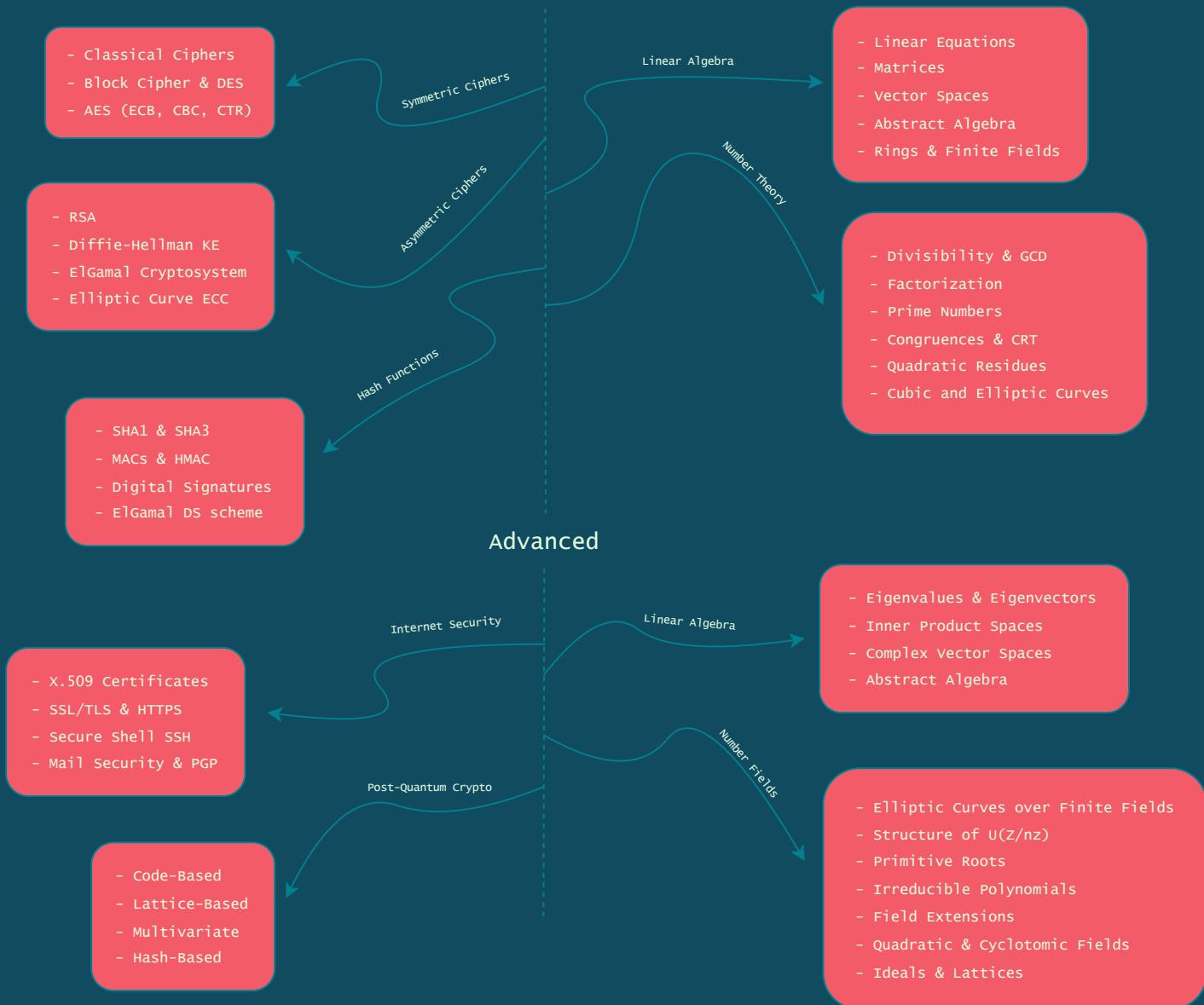
Books:
- Introduction to Linear Algebra with Applications by DeFranza.
- Linear Algebra Larson.
- Friendly Introduction to Number Theory.
- Algebraic Number Fields.
- Cryptography and Network Security.
- Serious Cryptography A Practical Introduction to Modern Encryption.

Note: The crypto content has to be studied in parallel with the related mathematics.

Made with ❤ by Ahmed Sayed @Y4mm1

2022