crypto

Provable security
https://en.wikipedia.org/wiki/Provable_security

Computational hardness assumption
https://en.wikipedia.org/wiki/Computational_hardness_assumption

Semantic security
https://en.wikipedia.org/wiki/Semantic_security

Polynomial time
https://en.wikipedia.org/wiki/Time_complexity#Polynomial_time

PP (complexity)
https://en.wikipedia.org/wiki/PP_(complexity)

Post-quantum cryptography
https://en.wikipedia.org/wiki/Post-quantum_cryptography

crypto people

Schneier on Security
https://www.schneier.com/

D. J. Bernstein
https://cr.yp.to/djb.html

ciphers

Block cipher
https://en.wikipedia.org/wiki/Block_cipher

Block cipher mode of operation
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Shor's algorithm
https://en.wikipedia.org/wiki/Shor%27s_algorithm ==> brute-force RSA

Stream cipher
https://en.wikipedia.org/wiki/Stream_cipher

RC4
https://en.wikipedia.org/wiki/RC4

padding

Padding
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Padding

https://stackoverflow.com/questions/2991603/pkcs1-v2-0-encryption-is-usually-called-oaep-encryption-where-can-i-confirm-i

https://en.wikipedia.org/wiki/PKCS_1

hash functions

SHA-3
https://en.wikipedia.org/wiki/SHA-3

Sponge function
https://en.wikipedia.org/wiki/Sponge_function

Message authentication code
https://en.wikipedia.org/wiki/Message_authentication_code

prng

Pseudorandom number generator
https://en.wikipedia.org/wiki/Pseudorandom_number_generator

Pseudorandom generator
https://en.wikipedia.org/wiki/Pseudorandom_generator

One-way function
https://en.wikipedia.org/wiki/One-way_function

Pseudorandom generator theorem
https://en.wikipedia.org/wiki/Pseudorandom_generator_theorem

Pseudorandom function family
https://en.wikipedia.org/wiki/Pseudorandom_function_family

/dev/random
https://en.wikipedia.org/wiki//dev/random

Hardware random number generator
https://en.wikipedia.org/wiki/Hardware_random_number_generator

arc4random – arc4 random number generator
https://man.dragonflybsd.org/?command=arc4random&section=3

random - random number devices
https://man.dragonflybsd.org/?command=random&section=4

random - random number devices
https://man.dragonflybsd.org/?command=random&section=3

Yarrow algorithm
https://en.wikipedia.org/wiki/Yarrow_algorithm

true randomness
https://www.random.org/

mac & ad

MAC
https://en.wikipedia.org/wiki/Message_authentication_code#Security ==> more on non-repudiation

Universal hashing
https://en.wikipedia.org/wiki/Universal_hashing

One-time pad
https://en.wikipedia.org/wiki/One-time_pad

Poly1305
https://en.wikipedia.org/wiki/Poly1305 ==> many more ssl libs there

ChaCha20 & Poly1305
https://datatracker.ietf.org/doc/html/rfc8439

A Security Analysis of the Composition of ChaCha20 and Poly1305
https://eprint.iacr.org/2014/613.pdf

NaCl (software)
https://en.wikipedia.org/wiki/NaCl_(software)

AEAD Algorithms
https://www.iana.org/assignments/aead-parameters/aead-parameters.xhtml

Authenticated encryption
https://en.wikipedia.org/wiki/Authenticated_encryption#Authenticated_encryption_with_associated_data_(AEAD)

UMAC: Fast and Provably Secure Message Authentication
http://fastcrypto.org/umac/

UMAC message authentication for SSH
https://datatracker.ietf.org/doc/html/draft-miller-secsh-umac-01

VMAC
http://www.fastcrypto.org/vmac/draft-krovetz-vmac-01.txt

key-exchange

Diffie–Hellman key exchange
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

mitm

MIG-in-the-middle

https://web.archive.org/web/20220312032816/https://www.dlab.ninja/2012/04/mig-in-middle.html

pkix

Public key infrastructure
https://en.wikipedia.org/wiki/Public_key_infrastructure

X.509
https://en.wikipedia.org/wiki/X.509

mitm-happy

HTTP Strict Transport Security
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

HTTP Strict Transport Security (HSTS) and NGINX
https://www.nginx.com/blog/http-strict-transport-security-hsts-and-nginx/

HSTS Preloading using Nginx, Letsencrypt and Capistrano.
https://dev.to/sonica/hsts-preloading-using-nginx-letsencrypt-and-capistrano-18l7

Setting up HSTS in nginx
https://scotthelme.co.uk/setting-up-hsts-in-nginx/

infosec

Information security
https://en.wikipedia.org/wiki/Information_security

anti-trojan

5 Tools to Scan a Linux Server for Malware and Rootkits
https://www.tecmint.com/scan-linux-for-malware-and-rootkits/

sniffing

How do I use SSH Remote Capture in Wireshark
https://ask.wireshark.org/question/2506/how-do-i-use-ssh-remote-capture-in-wireshark/

videos

DEF CON 19 - Moxie Marlinspike - SSL And The Future Of Authenticity
https://www.youtube.com/watch?v=UawS3_iuHoA