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)

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

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

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

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

hash functions

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

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

key-exchange

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

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/