# Secret Key Cryptografie

DES: Data Encryption Standard

AES: Advanced Encryption Standard

IDEA: International Data Encryption Algorithm (precies nie meer als alln afk gezien)

Number cruncher 🡪 zelfde functie veel x na elkaar uitvoeren

Block cipher 🡪 verdeeld in blokken (bv. van 64 bits)

RSA: Rivest, Shamir, Adleman (=de namen van die kerels)

PKI: Public Key Infrastructure

CA: Certification Authority

DN: Distinguished Name

RA: Registration Authority

VA: Validation Authority

CRL: Certificate Revocation List: lijst van certificaten die vervallen/ingetrokken zijn of gehackt zijn.

OCSP: Online Certificate Status Protocol: protocol om aan een reeks servers die aan load balancing doen te vragen of een certificaat nog geldig is. (deze hebben de CRL blacklist)

CP: Certificate Policy

CPS: Certificate Practice Statement

TTP: Trusted Third Party

PGP: Pretty Good Privacy (secure e-mails)

S/MIME: Secure Multipurpose Internet Mail Extension

WoT: Web of Trust

SSL: Secure Socket Layer

TLS: Transport Layer Security

MAC: Message Authentication Code 🡪 controllegetal 🡪 hash van key + message (= soort hashing met zelfde voorafgesproken salt tussen A en B)

VPN: Virtual Private Network

PPTP: Point to point Tunneling protocol

# Beveiliging

ACL: Access Control List

WLO: WildList Organisation

BSI: Boot Sector Infectors

(VBR: Volume Boot Record)

RAT: vroeger 🡪 Remote Access Tool, nu 🡪 Remote Access Trojan

(SSDT: System Service Descriptor Table)

TCP (om hem toch nog mr der tussen te zetten): Transmission Control Protocol

ARP: Address Resolution protocol

DoS: (allé wie kent die nu nie)

DHCP: Dynamic Host Configuration Protocol

DNS: Domain Name System

POD: Ping Of Death

DDoS

CVE: Common Vulnerabilies and Exposures

IDS: Intrusion Detection System 🡪 HIDS voor hosts, NIDS voor netwerk

IPS: Intrusion Prevention System

Fuzzy Rules 🡪 Statistical berekeningen om met verschillende waardeverhoudingen rekening te houden (Anomalue-gebaseerde IDS)

LM: Log Management

TTP: Trusted third party

SIEM: Security Information and Event Management

SIM: Security Information Management

SEM: Security Event Management

XSS: Cross-site scripting