Simple Ciphers

Shift cipher: letters as numbers, modular shift by constant factor
Transposition cipher: key is permutation of letter position
Substitution cipher: swap character sequences around according to known mapping
Vigenere cipher: shift cipher with multi-letter repeated key

Security

Computational or unconditional

$$p_C(C) = \sum_K p_K(K) p_P(D(K,C))$$

$$p_C(C \mid P) = \sum_{\{K|P=D(K,C)\}} p_K(K)$$

$$p_P(P \mid C) = \frac{p_P(P) p_C(C|P)}{p_C(C)}$$

$$= \frac{p_P(P) \sum_{\{K|P=D(K,C)\}} p_K(K))}{\sum_K p_K(K) p_P(D(K,C))}$$

Unconditional: $p_P(P \mid C) = p_P(P)$

Crypto.

Fixed/variable length input random functions
Pseudo-random function: deterministic, efficiently computable, cannot be distinguished by practical statistical/cryptanalytical test from a random function
Random sources: hardware, user behaviour, timing of peripheral, A/D noise, network timing, high-resolution time

Secure Hashes

Preimage resistance: for given y, cannot find x st. h(x) = y
Second preimage res.: for given x, cannot find x' st. h(x') = h(x)
Collision resistance: cannot find x != y st. h(x) = h(y)
Based on fixed input length PRF called a "compression function"
Input bitstring X padded by 1, then filled to block width by 0
$H_i = C(H_{i-1} \| X_i)$, fixed H_0
Birthday: k balls, n bins, prob. bin have 1 ball: $\frac{n!}{k!n^k}$, $k = \sqrt{n}$

MAC

$MAC_K(M) = h(K \| M)$, but vulnerable to message extension attack with compression-h

Hash Chain

$R_i = h(R_{i-1})$, random R_0, then store R_n in server, Rs to clients. Client sends R_{i-1} and server compares hash of to its R_i

Prior Knowledge

Publish h(M) for your M, possibly h(N||M) for small M

Hash Tree

Leaves contain message hashes, branches hashes of subhashes

One Time Signatures

Have secret keys 2n random R_{ij}, public key 2n $h(R_{ij})$: signature $(R_{b1,1}, R_{b2,2}..)$ for b in h(M)

Stream Auth.

Verify each packet immediately, but don't sign each message: have $C_i = h(C_{i+1}, M_i)$ then send C_1,Sig(C_1),(C_2,M_1),..,(0,M_n)

Blockcipher

Key dependent permutation
Confusion, diffusion

Feistel Structure

$P = L_0 \| R_0$, $R_i = R_{i-1} \oplus f(L_{i-1})$ (odd) $L_i = L_{i-1} \oplus f(R_{i-1})$ (even)
Need at least 3 rounds for rnd.
DES: 16 rounds, 56 bit key, 64 bit block, f uses XOR of scheduled key with block through S-boxes
Triple DES:

$$E(X) = DES_{K3}(DES_{K2}^{-1}(DES_{K1}(X)))$$

ECB

Cut message into n-bit blocks and encrypt separately: bad since patterns + input alphabet is limited (plaintext ASCII only)

CBC

$C_i = E_K(P_i \oplus C_{i-1})$, random C_0

MAC

As CBC, but no C_0 and transmit only last C: can verify message if you know the secret key

Hash From Blockcipher

$H = X \oplus E_K(X)$

$H_i = H_{i-1} \oplus E_{X_i}(H_{i-1})$

Random Bit Stream

$R_i = E_K(R_{i-1})$, replace K before $2^{\frac{n}{2}}$ numbers have been made

OFM

As above, $R_0 = 0$, $C_i = P_i \oplus R_i$

CTR

$R_i = E_K(i + O)$, $C_i = P_i \oplus R_i$, could transmit O with message

CFB

$C_i = P_i \oplus E_K(C_{i-1})$, random C_0

Diffie-Hellman

Large prime p, g $\in Z_p^*$, A B generate x, y < p – 1. Now: A⇒B: g^x mod p, B⇒A: g^y mod p, each uses $h(g^{xy})$ as shared key

EIGamal

A publishes (p, g, g^x) and keeps x. Now: B⇒A: (g^y mod p, (g^{xy}M) mod p) and A calculates $[g^{xy}M][g^{y(p-1-x)}]$ mod p = M

EIGamal Signature

A generates y and solves xg^y+ys = M (mod p) for s, then certificate is (M ,g^y mod p, s). B

	can then test equation raised to the power of g on both sides
PKI	Certificate authority issues $Cert_C(A)=\{A,K_A,T,L\}K_c^{-1}$, where C confirms K_A belongs to A for T to T + L: anyone who knows K_C can verify this. Now can establish chain of trusted certificates
Passwords	Reject delay, monitor failure, password strength, randomness
Challenge Response	$A \Rightarrow B$: N $B \Rightarrow A$: $h(K_{ab}\|\|N)$ or $\{N\}_{Kab}$
Mutual Challenge Response	$A \Rightarrow B$: N_a $B \Rightarrow A$: $\{N_a,N_b\}_{Kab}$ $A \Rightarrow B$: N_b Has attack where new session to A can be used to authenticate a B who does not know K: make K_{ab} different from K_{ba}
One Time Key	$B \Rightarrow A$: C,$\{C\}_{Kab}$, C increases
Generating Key	Card A_i has I, $K_i = \{i\}_K$. Now: $A_i \Rightarrow B$: i, $B \Rightarrow A_i$: N, $A_i \Rightarrow B$: $h(K_i\|\|N)$
Key	Only one K, store in every device
Kerberos	$A \Rightarrow S$: A,B $S \Rightarrow A$: $\{T_s,L,K_{ab}, B, \{T_s, L, K_{ab}, A\}_{Kbs}\}_{Kas}$ $A \Rightarrow B$: $\{T_s,L,K_{ab},A\}_{Kbs}$, $\{A, T_a\}_{Kab}$ $B \Rightarrow A$: $\{T_a+1\}_{Kab}$ Trusted third party, tickets have lifetime and timestamp, limit use
Discretionary Access Control	Owners have discretion how they want to share their objects: identity based access
Mandatory Access Control	System wide policy based access, e.g. prevents certain information flows. Enforced without owner consent
UNIX	User, group, outher bits SUID: effective, real and saved (initial effective) UIDs/GIDs Directories: read = list, write = remove files/empty dirs, execute = traverse, sticky = whether write is sufficient to delete files in the directory
Windows	Access control lists stored with owner with object, object types have their own permission lists
Principle Of Least Priv.	Implemented as transferable capabilities: combine the notion of a reference and rights
MAC Policy	Air gap security Data pump/diode Bell/LaPadula: subjects and objects have confidentiality labels, system prevents flow from high to low level objects, trusted subjects can override Covert channels: resource conflicts, timing, resource state
Commercial Integrity	Internal consistency (checked automatically), external consistency (describes the real world) Constrained Data Items only accessed via Transformation Procedures: certify TPs, some TPs can convert UDIs, all must log sufficient audit information Integrity Verification Procedures for every CDI Require authentication for subjects and checks on (subject, TP, CDI) triplets before allowing execution
TCB	The parts of a system that enforce a security policy and whose correct operation is sufficient to ensure enforced
OS Security	Domain separation: protect TCB from external interference Reference mediation: accesses by untrusted subjects must be validated by the TCB Residual information protection: when allocated or deallocated
Security Classification	DoD Orange Book. D: no auth, C1: discretionary, C2: auditing, ACLs, B1: labels, tests, B2: formal security policy, identify covert channels, B3: security alarms, minimal TCB, A1: formally verified design
Vulnerability	Viruses spread where binary programs are exchanged and writable by other programs Checks for data size, data content, boundary conditions, missing locks, race conditions, environment checks, auth.
Networks	Protocols not designed for hostile environments, bus and broadcast technologies, DDOS TCP: start sequence number acts as authentication nonce

SYN flood: local buffer allocated for every SYN packet
DNS: cache unsolicited query
Firewall: matches sets of IPs / port numbers, plausibility check on source IPs, logs + audits, but no protection against insiders or tunnels, disrupts deployment of new protocols

Security Policy Construction

1. Identify assets + value, vulnerabilities, threats, legal requirements, priorities
2. Work out suitable policy: first high level security policy that clarifies what are authorised, required and prohibited activities, states and information flows
3. Document high level policy in security policy document: reference for implement.
4. Select and implement controls: general responsibilities, overall responsibility for maintenance, enforcement, review, owners for individual information assets, reporting responsibilities, process review, disciplinary action, incentives, user training, personnel security, physical security, segregation of duties, auditing, backup, media disposal, encryption etc….

Computer Misuse

Causing a computer to perform a function with the intent to access without authorization
Unauthorised modification to impair operation / hinder access

DPA

- Fairly + lawfully proc.
- Proc. for limited purps.
- Adequate, relevant
- Accurate
- Not kept for longer than necessary
- Processed in accordance with subject rights
- Secure
- Not transferred to countries without prot.