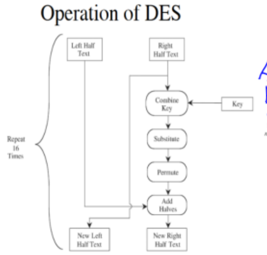
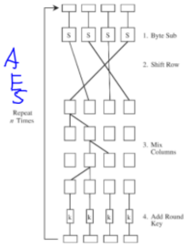
Crypt Sheet Daniel Willard CS 433 CH 1-6

1)Confidentiality Integrity Availability Authentication Accountability (CIAAA**) Defense**: prevent, deter, deflect mitigate, recover **Controls**: Encryption, Physical, Hardware (firewalls, auth/intrusion devices), Software, Policies. **2)Caesar cipher**: assign the values to the character and shift them on a sliding scale. One-time Pads: $c_i = (p_i+k_i)$ mod 26, Large, non-repeating keys(k) written on sheets(p_i) of paper glued into a pad **Vernam Cipher**: single large key of non-repeating numbers (use exclusive OR) **Transposition/permutation**: Rearrange letters of plaintext. **Product Cipher**(use serval ciphers) **Stream and block**: convert symbol by symbol Block encrypts groups of symbols. **DES**: standard arithmetic and logical operations are used Implementable in both SW and HW. **AES**: Symmetric block cipher 10, 12, 14 rounds (128,192,256) Substitution, transposition, shift, XOR, addition. **RSA**: Key Choice (n, e, d) Encryption key: (e, n) Decryption key: (d, n) n = p * q, where p and q are large prime numbers, **e** is relatively prime to (p-1)*(q-1), Select d such that e*d = 1 mod (p-1)*(q-1).


Operation of DES



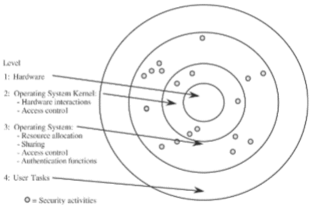
$p = 5, q = 3, n=15. \ (p-1)*(q-1)=8$

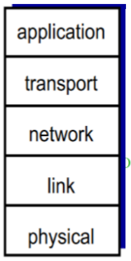
Choose $e=11$ and $d=3$.

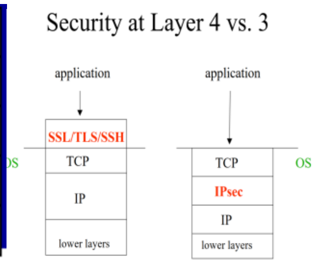
$P=2$

$C=P^e \bmod n = 2^{11} \bmod 15 = 2048 \bmod 15 = 8$

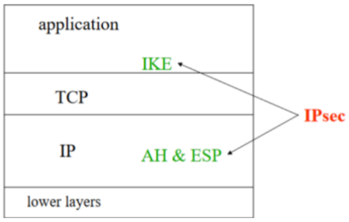
$P=C^d \bmod n = 8^3 \bmod 15 = 2$

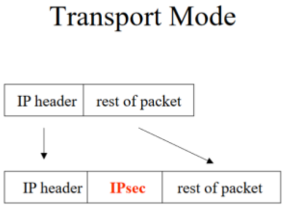


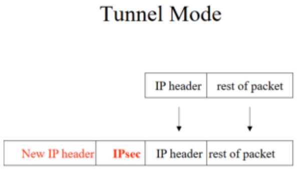


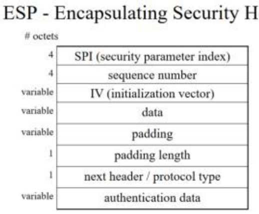

Security at Layer 4 vs. 3

Authentication: Knows(p-word)Has(id,key)is(bio). **Attacks**: dictionary attack, inferring, guessing, defeating concealment (find the table) Exhaustive. **Bio**: false pos, False neg, intrusive, costly. **Federated Identity Management**: (sin into FIM then no auth needed) unifies the ID and auth process for a group of systems. **Single Sign-on**: (sign into SSO then acts out auth needed) Umbrella task acts on behalf of user. Access **Control Matrix**: column object(file) row subject(user) **Access control list(col)**: one access control list per object(file to userList) **Directory(row)**: directory per user (per subject) **Capability:** A ticket giving permission to a subject to have a certain type of access to an object**. Procedure-Oriented**: Must go through a specific procedure to access an object**. Role-Based**: Associate privileges with roles.**3) Nonmalicious Errors**: Buffer overflows, Incomplete mediation(can user do that?), Time-of-check to time-of-use(synchronization/race) **Malicious Code(apps, memory, boot sector)**: **Virus** (replicate itself, pass on malicious code mod prog) {**Transient**: runs with host prog. **Resident**: in memory always running}, Trojan horse: primary effect + nonobvious malicious effect, Logic bomb: boom on specified condition, **Trapdoor/backdoor**: a program's nonobvious access point. **Worm**: self-spreads in network**, Rabbit**: self-replicates endlessly. **Detection:** must be stored somewhere searches memory and disk, monitors execution, and watches for virus signatures. Polymorphic V's: Randomize locations, fixed data, keys, insert no-ops instructions.**5)OS SEC**: mem, I/O, Network, Programs, data. **Methods**: Separation virtual/physical/Temporal/logical(user operates under illusion of no process are running)\cryptographc**. Levels**: None/Isolate/Share all/none/ Discretionary (user control objects)/ Mandatory (O.S. control access to objects) / limit use of object. Memory: holds limits though fence, relocations, base\bound, segmentation. **Features**: ID, auth, MAC, DAC, Object reuse protection, Complete mediation, Trusted path, Audit, Intrusion detection**. Bell-La Padula Confidentiality**: Security class C(s) C(o)(military rank, clearance) read only if C(s) ≥ C(o)(read up) can write to p only if C(o) ≤ C(p)(write down). **Biba Integrity** : modify only if I(s) ≥ I(o), write object p only if I(o) ≥ I(p). **Graham-Denning** : control matrix (Create object, create subject, delete object, delete, Subject, Read access right, grant access right, delete access right, transfer access right). **Harrison-Ruzzo-Ullman**: if A has condition, then op. if commands are not restricted to one operation each, it is not always decidable whether a given protection system can confer a given right. **Take-grant**: create, revoke, grant, take. **Design**: layered design, Kernelized design(security), Separation/Isolation, Virtualization, least privilege, Open design, Economy of mechanism, Permission based, Separation of privilege, Least common mechanism. **6) NETSEC routing(map it)/forwarding(send it)**: Local/wide area network, ISP{ Internet Exchange point (connect ISP, Border Gateway Protocol},Nodes, links**. Threats**: interception ,Modification change packet, Fabrication(sequencing, substitution, insertion, replay) make packet, Interruption(Routing, Excessive, Component failure) (anonymity, vast, sharing, complexity, unknown path/perimeter. **WIFI:** weak protocol, available, accessible, pt transit. DOS: ping flood, Smurf echo, DNS spoof, session hijack DistroDOS. **Link Layer**: E2E message encrypted not path. LinkE, path encrypted not message, VPN. **NET layer**: IPSEC IPsec authentication cannot distinguish between users (transparent to apps), RoutingSEC control plane (sign it). **4Level:** no way to notify TCP layer if data is bogus. IPSEC: Secure channel though **E, anti-replay,** connectionless Integ, auth on IP address, enforced access control. **AH&ESP**: IP header extensions for carrying cryptographically protected data. **IKE:** A protocol for establishing security associations session keys, not req. Modes: Tunnel, Transport. **TSL/SSL**: Secure Socket Layer, Transport Layer Security Calculate hash(K, (m1, m2, "CLNT or SRVR") create: write, read, integrity, E keys and IV. **Firewall**: filter by packet, stateful, app, personal. Intrusion: signature vs anomaly/ host vs network.

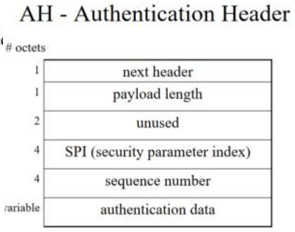



Transport Mode

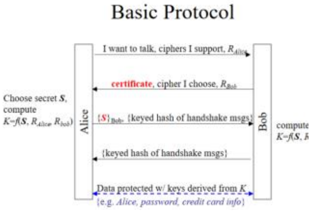

Tunnel Mode


ESP - Encapsulating Security Head

# octets	
4	SPI (security parameter index)
4	sequence number
variable	IV (initialization vector)
variable	data
variable	padding
1	padding length
1	next header / protocol type
variable	authentication data


AH - Authentication Header

# octets	
1	next header
1	payload length
2	unused
4	SPI (security parameter index)
4	sequence number
/ariable	authentication data


Basic Protocol
I want to talk, ciphers I support, R_{Alice}
certificate, cipher I choose, R_{Bob}
Choose secret S, compute $K=f(S, R_{Alice}, R_{bob})$
Alice
$\{S\}_{Bob}$, {keyed hash of handshake msgs}
Bob
compute $K=f(S, R$
{keyed hash of handshake msgs}
Data protected w/ keys derived from K
{e.g. Alice, password, credit card info}