Recall the notation that x || y means the concatenation of x with y, {x}k denotes the encipherment of x using key k, h(x)denotes a hash of x, and MAC K{x} demotes MAC of x with key K. **Cipher –** Cipher is algo to encrypt or decrypt text -> creates cipher text **Sub –replacecharvsperm.**

**Columnar Transposition –** key up top ordered by alphabet and do list by row then list out by column.

Main components of security Confidentiality/Privacy data are only available to the appropriate parties, which may be parties that require access to the data or parties that are trusted. confidential data are not disclosed to people who do not require them or who should not have access to them. Ensuring confidentiality means that information is organized in terms of who ought to have access as well as its sensitivity.

**Stream –** faster than block, char by char no need to wait for block **Block -**  building blocks of crypto tools, otp, hash func, MACs

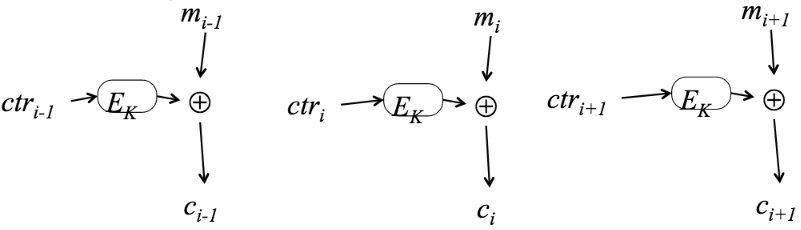
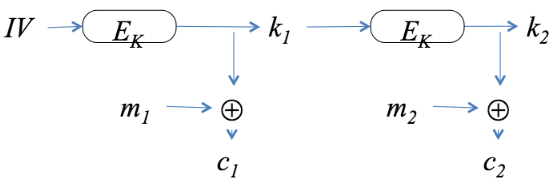
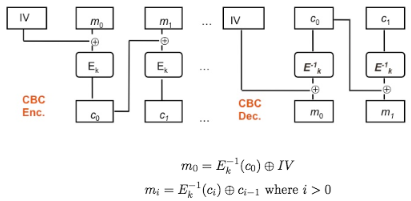
**AES –** Clear replacement for DES. Faster than 3DES. Private Key Symmetric block ciper 128-bit Data, 128/192/256-bit keys. Stronger than 3DES. 20-30 year life. Security, implementation ease, flexibility, computational cost, simple design. Efficient on 8-bit CPU.

**Integrity/Authenticity** Data integrity refers to the certainty that the data are not tampered with during or after submission. It is the certainty that the data will not be modified or destroyed by unauthorized parties. This means there are two points during the transmission process during which the integrity could be compromised: during the upload or transmission of data; during the storage of the document in the database or collection. **Availability** This means that the information is available when it is needed. In order for a system to demonstrate availability, it must have properly functioning computing systems, security controls and communication channels. **Non-repudiation/Accountability** authorof a statement will not be able to successfully challenge the authorship of the statement or validity of a document **Threat**: Potential of attack **Attack**: …an attack **Vulnerabilities**: Weakness that make things susceptible to attacks **Control**: action taken to remove vulnerability **Attack Surface**: Places that attacks can occur

**Security Strategy**: **Policy**: statement of what is or not allowed b. **Mechanism**: method for enforcing policy

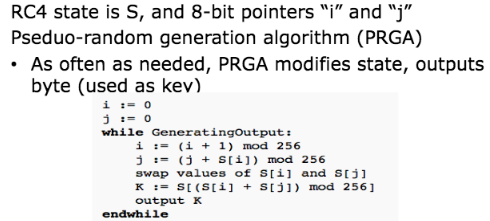
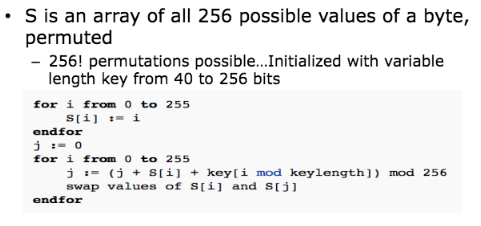
**Security Principles**: 1. **Economy of Mechanism** - Keep the system design simple 2. **Fail-Safe defaults** - Default is lack of access 3. **Complete Mediation** - Everything gotta be checked 4**. Open Design -** Security is not based on hidden 5. **Least Privilege** - minimum privilege to do task 6. **Separation of Privilege** 7. **Least Common Mechanism –** don’t share mechanism between users 8. **Psychological Acceptability -** Easy to use

**ECB, Cipher Block Chaining** – Self-healing (at most two blocks) **Output Feedback –** losing sync is fatal, needs IV **Counter –** Gen bit in middle of stream -> operate on blocks in parallel.



**Stream cipher** try to implement one-time pad by xor key with message

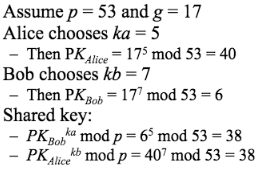
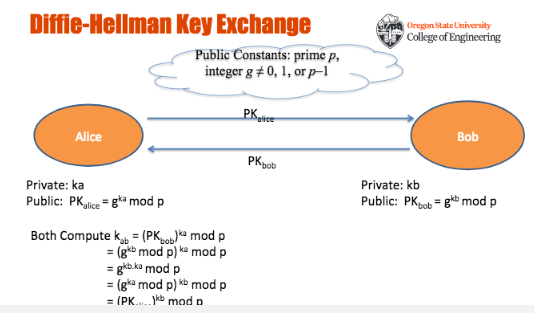
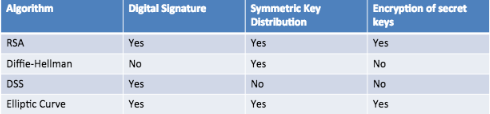
**RC4/” Keystream –** stream cipher used in SSL/WEP. Period of 10^100. Variable keylen 1-256. Byte operation. Efficient. Array S stores all possible values 0-255. 256! Permutations possible. Variable length key 40-256 bits.

 ../../../Desktop/Screen%20Shot%202017-10-25%20at%202.19.28%20AM.png

**Public Key Crypto:** Two keys, public and private. **Usage:** Confidentiality – encipher w/ public Authentication – encipher w/ private

**Req:** comp easy to generate key pair, comp easy to encrypt using public key, comp easy to decrypt w/ priv key, comp infeas to get priv key from public key, comp infeas to recover original msg from pub key and ciphertxt, both key can be used encrypt/decrypt.

**Stats**: much slower than symmetric: RSA 100-1k slower than DES, 10k slower AES. Gen. used in conjunction with sym system for bulk encrypt. Based on hard problems (factoring composite primes, discrete log, elliptic curves). Small # of pub key perform encryption and sign.

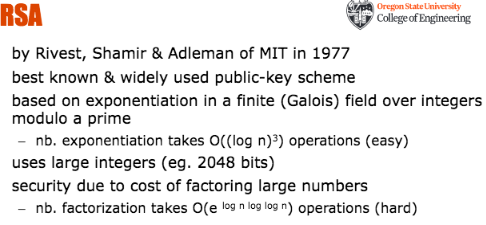
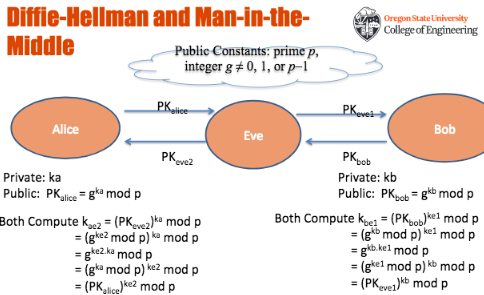
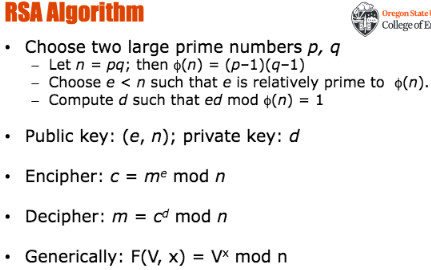
**Diffie-Hellman –** first public key cryptosystem used to compute common shared key. Based on disc log problem. 

**Totient Function φ(n)** – Number of pos integers less than n and relatively prime to n (no common factors)

**RSA: confidentialiity** m^e mod n = c, **authentication/integrity** m^d mod n = c, **Both** (m^d mod n)^e = c

**Avalanche Effect:** flip one bit half are flipped. Differ by 5 bits how many bits differ in final n/2 bits.

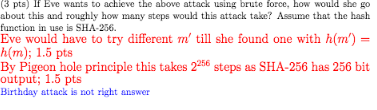
**AES –** faster than 3des, larger key space, larger block size (same key can encrypt more before the key needs to be changed)

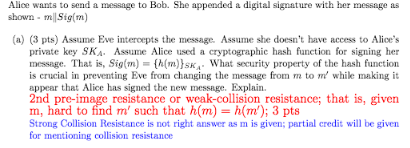


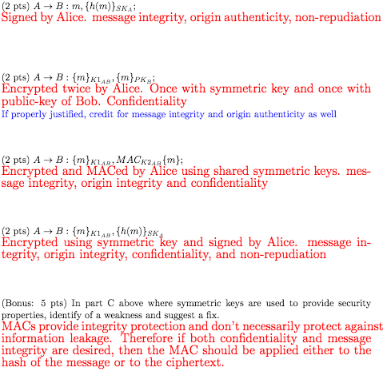
**brute force 2DES** 2^56 \* 2 or 2^57**. Hash function** should have at least 2K output bits, w/ encryption algo of key len K.

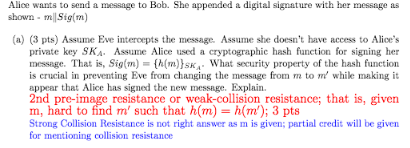
**Algo to generate hash** is SHA-2 or RSA. **Hash function** is not crypto secure if output bits so large that collision is impossible.

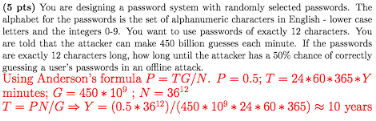
Birthday attacks are ineffective against keyed crypto hash functions such as HMACS. **Encoding Vignere cipher** with multiple keywords add all numbers together and mod 26.











Des no longer secure 2^56 too small for modern computers. Exhaustive search easily done. Encryptx3 mode is 112 bits. DES only uses 64 bit block size and AES uses 126 bit block size.

Properties of IV depend on the cipher and the mode it is being used for. At a minimum IV should be unique for every invocation with the same key. Otherwise the mode may devolve into ECB mode where the same plaintext message will result in the same ciphertext. In some cases random or unpredictable IVs may be desirable. Typically IV need not be kept secret but its integrity should be protected. Don’t fix IV ahead of time, same as ECB.

Yes, it is feasible to convert a block cipher into a stream cipher. Cipher feedback mode, output feedback mode and counter mode all convert a block cipher into a stream cipher.

**3 components crypto hash –** Pre-image resistance, Weak-collision resistance, Strong-collision resistance. **Weak-collision –** given x find x’ such that h(x) = h(x’) and x =/= x’. **Strong-collision –** pick x and x’ such that h(x) = h(x’) and x =/= x’. Strong implies weak and weak implies pre-image resistance. **Birthday attack – hash function maps inputs to a 32 bit hash** 2^(n/2) attack higher likelihood of collisions between random attack attempts and fixed degree of pigeonholes. **Security of public key** crypto schemes can be reduced to the difficulty of solving-well known hard problems. **For alice to sign** – {K||MSG} pk\_b, {h{K||MSG}pk\_b}} sk\_a. **Really long msg,** bulk of msg gen with random gen symmetric key and transmitted with public key – {K} p\_B, {M}k, {h(M)}sk\_a. Last block for integrity protection. **Digital sig vs MACs** – MACs can be used to protect integrity of msg (not tampered with) and provide authenticity of origin. Only they share key so no repudiation. Digital signatures can also protect the integrity of the msg and provide authenticity of origin. Sent using a key only signer has so proves that they sent the message. **Man in middle** – Attack where person sits in middle **vs. Meet** brute force attack from both ends to trade comp effort with space. **Important to hash msg for dig sig –** RSA sig on m1 without hash function S1 = (m1)^d mod N. Someone who has access to signatures on m1 and m2 can produce sig on m1\*m2 wihtout access to key S1 \* S2 = (m1)^d mod N \* (m2)^d mod N = (m1 \*m2)^d mod N = Sign on m1 \* m2. Hash function prevents problems and reduces computational effort. Signing hash is less expensive than sign entire msg.