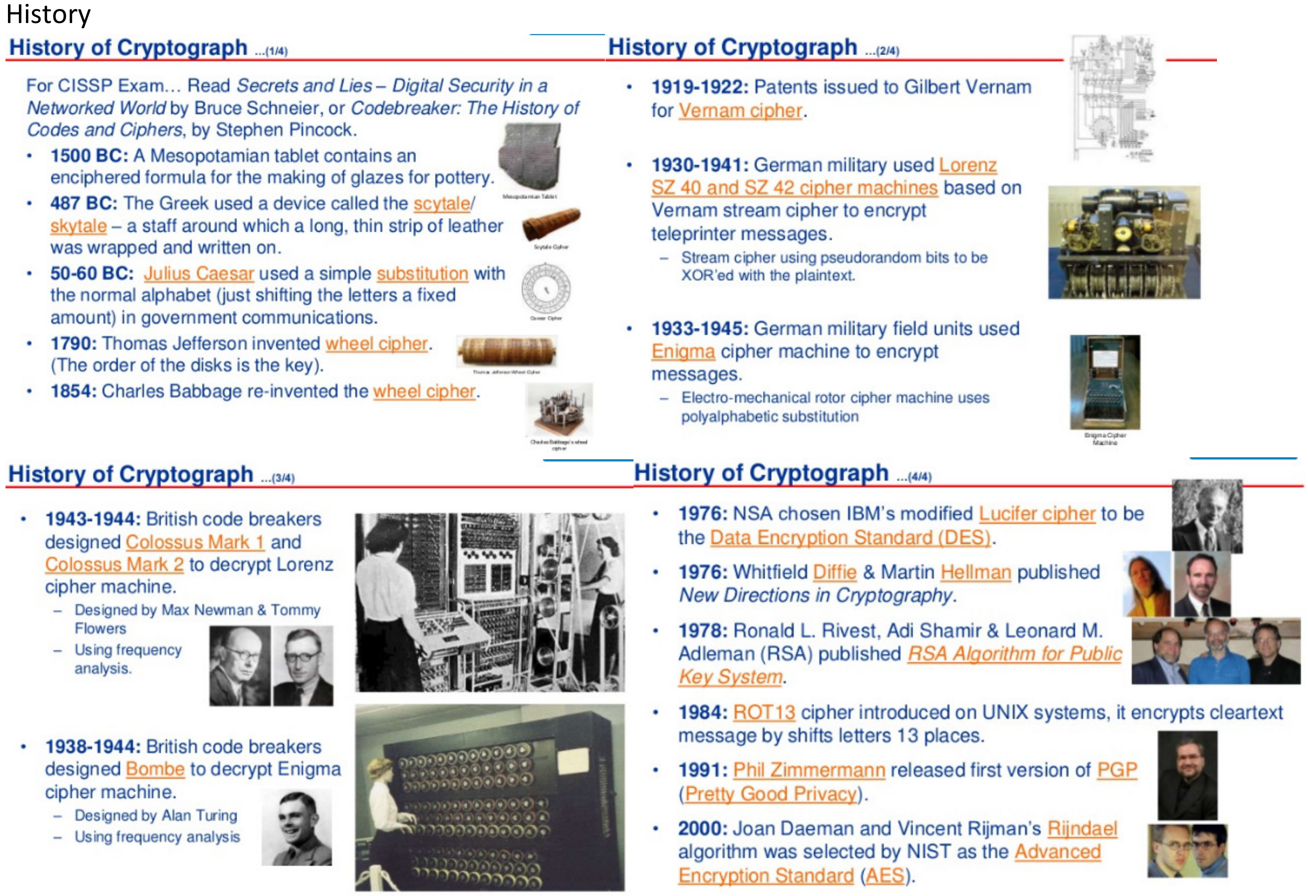
Cryptography – Summary of Notes & Learnings – by Arvind Mathur (10-Dec-2016)

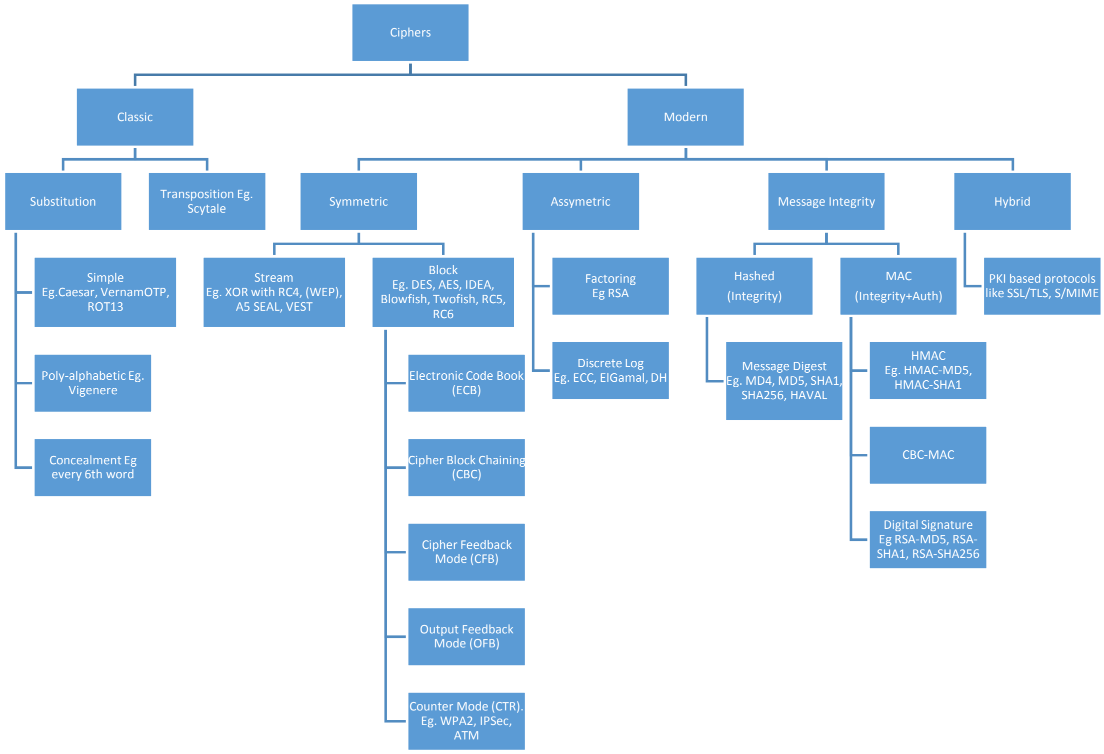
* Thanks to number of sources for excellent slides/ visuals

1. General Notes
   a. Kerckhoff's Principle – only protect the key. The algo should be public knowledge
   b. Strength of cryptosystem – Algo + secrecy of key + length of key + IV + operations
   c. Services of Crypto – Confidentiality, Integrity, Authentication, Authorization, Non-Repudiation
   d. Strength depends on: Substitution, Transposition, S+P (in block), Diffusion, Confusion
   e. Goal is to increase work-factor – that dissuades an attacker to go look for easier prey

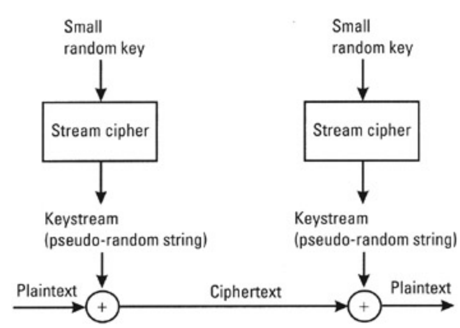
2. History



3. Cipher Types



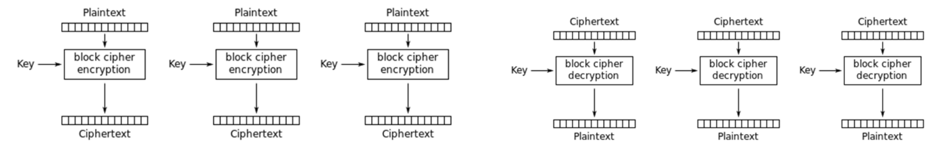
4. Methods of Encryption
   a. Symmetric
      i. Basics
         1. Single/secret key – encrypts and decrypts
         2. Fast and Hard to break
         3. Large number of keys required – n*(n-1)/2
         4. Confidentiality only. + MAC for integrity and auth
      ii. Stream
         1. Essentially a substitution cipher, where a random keystream is used to XOR the PT to generate the CT in real time
         2. Very fast, often Hardware implemented
         3. Stream generator is the key. Key must be long, non-repeating, unpredictable, unbiased
         4. If implemented well, is super strong. But badly can be weak
         5. RC4 (from RSA) is popular – in WEP, SSL/TLS



      iii. Block
         1. Blocks of 64, 128, 192 bits at a time. Can operate in stream mode to handle longer data
         2. Combines Substitution and Permutation/ Transposition – stronger than Stream, but more computationally intensive so software based
         3. Initialization Vector to add unpredictability and diffusion

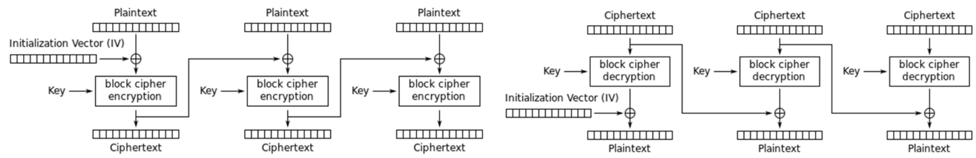
4. Block Cipher Modes – to securely encrypt PT greater than block size

Electronic Code Book (ECB)
Each block encrypted exactly the same. Good for random access message, but for large messages, can fall prey to Known Plaintext, Replay Attacks or Linear Cryptanalytic attack



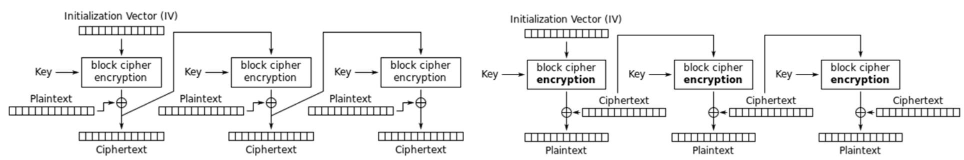
Electronic Codebook (ECB) mode encryption   Electronic Codebook (ECB) mode decryption

Cipher Block Chaining (CBC)
XOR with IV or prev CT before encryption.
Need to be used in full block mode so padding is required. To decrypt prev CT is used to XOR, so **errors don't propagate**. Encryption must be serial, but decryption can be parallel.



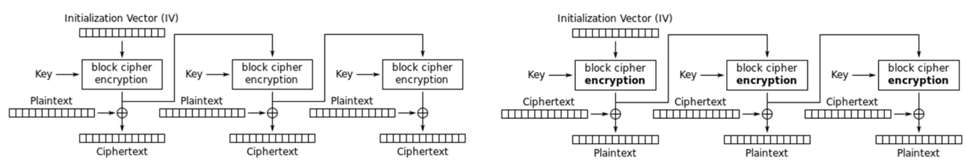
Cipher Block Chaining (CBC) mode encryption   Cipher Block Chaining (CBC) mode decryption

Cipher Feedback (CFB) – effectively steam. Each bit in keystream is CT(CTprevious).
Close relative of CBC – self- synchronizing stream cipher (loss of some CT has limited impact).



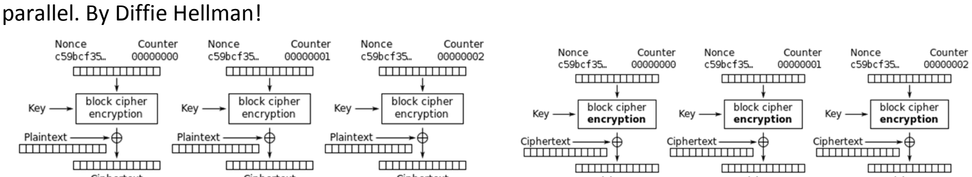
Cipher Feedback (CFB) mode encryption   Cipher Feedback (CFB) mode decryption

Output Feedback (OFB) – effectively steam. Keystream is CT(Keystream previous). Cannot be encrypted or decrypted in parallel.



Output Feedback (OFB) mode encryption   Output Feedback (OFB) mode decryption

Counter (CTR) – effectively steam
A 64 bit random data block used as first IV. Initially questioned, but now one of the most commonly used (WPA2 – AES + CBC-MAC). Counter is like stream generator – so can work very fast and in parallel. By Diffie Hellman!



Counter (CTR) mode encryption   Counter (CTR) mode decryption

5. Data Encryption Standard – Based on IBMs Lucifer ~ 1977
   a. 64 bit block Feistal (breaks 64 bit into 2 X 32) with 56 bit key
   b. 16 rounds of S&P
   c. Too easy to break – in a few mins with modern computers
6. AES – NIST selected Rijndael in 1997. Others RC6, MARS (IBM), TwoFish
   a. 128 bit block cipher with 128, 192, 256 bit keys
   b. Variable number of rounds with 4 steps. Round Key
   c. Counter Mode with Cipher Block Chaining Message Auth Protocol (CCMP) is part of 802.11i for WiFi. Based on AES using CTR (for confidentiality) with CBC-MAC (for integrity).

7. Blowfish – by Bruce Schneier, lightweight Festal type, upto 448 bit keys
8. Twofish – also by BS, finalist for AES
9. RC5, RC6 – by Ron Rivest of RSA. Upto 2040 bit keys. Upto 255 rounds
10. Comparisons

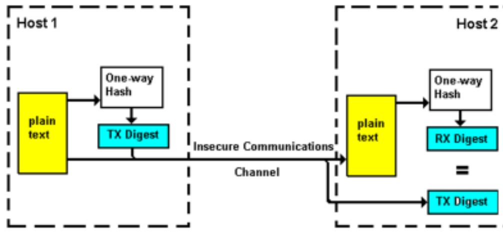
	Symmetric Encryption Algorithms			
	DES	***TDES***	***AES***	***BLOWFISH***
Block Size	64 bit	64 bit	128 bit	64 bit
Key size	56 bit	168 bit	128,192, 256 bit	32-448 bit
Created By	IBM in 1975	IBM in 1978	Joan Daeman in 1998	Bruce Schneier in 1998
Algorithm Structure	Fiestel Network	Fiestel Network	Substitution Permutation Network	Fiestel Network
Rounds	16	48	9,11,13	16
Attacks	Brute Force Attack	Theoretically possible	Side Channel Attacks	Not Yet

b. Asymmetric
   i. Basics
      1. Public Key and Private Key
      2. Confidentiality – encrypt with public key of receiver
      3. Open Message/ Proof of Origin – encrypt with private key of sender
      4. PoO+Conf – encrypt w/ private key of sender then public of rec
   ii. Factoring – RSA – factoring 2 large prime numbers. Basis for PKI.
   iii. Discrete Logarithmic
      1. Diffie-Hellmann – discrete logarithm (DL) key exchange algorithm to negotiate secret symmetric keys for subsequent symmetric encryption. Used in PKI.
      2. El Gamal – Diffie-Hellmann+ confidentiality + Digital Signature. Slow
      3. Elliptic Curve Cryptography (ECC) – highest strength per bit of key length – easier on computing and bw. Used in smart cards, wireless etc.
   iv. Advantages – not just confidentiality, but also: Non-Repudiation of Origin, Access Control, Data Integrity, Non-Repudiation of Delivery
   v. PKI Infrastructure
      1. ISO standard (X.509) – Programs, data formats, procedures, protocols, policies, cypto mechanisms – working together.
         a. Certificate Authority – Provides digital certificates – including identity and public key. CAs need to be cross-certified. Can revoke, expire, renew certificates
         b. Digital Certificate – link public key to components that uniquely identify the owner – based on X.509
         c. Registration Authority – verifies identity for CA
         d. Certificate Repository, Revocation system
         e. Key Backup & recovery system (escrow), Key history
      2. Trusted Platform Module (TPM) - chip on MB – dedicated to storage & processing of symm/asymmetric keys, hashes, and digital certificates
         a. Key wrapping
         b. Disk binding to motherboard (hashing)
         c. Sealing system state to hardware/ software config (Hashing)

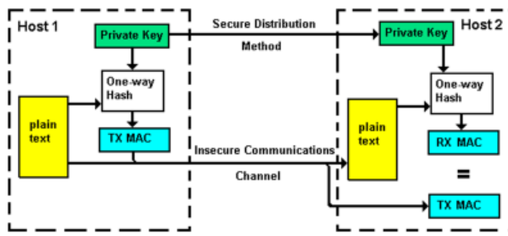
c. Message Integrity

i. Parity/CRC checks only work for unintentional integrity issues. To circumvent intentional/ malicious integrity issues, MI protocols were designed.

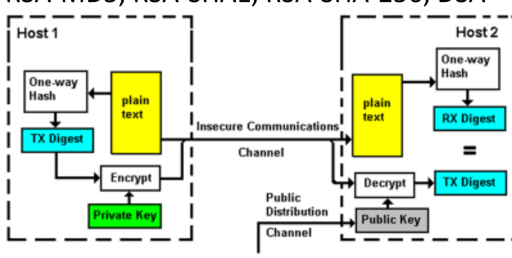
1. One-way code (smaller than message). Needs to be collision-free: No two messages create same hash
2. Hash – no keys. Only provides integrity check for unintended errors
   a. MD4 (old), MD5 (128b), SHA-1 (160b), SHA-256 (256b), SHA-3 (2012), HAVAL (upto 256b)



3. Message Authentication Code – Message + Key = authentication
   a. HMAC – HMAC-MD5, HMAC-SHA1, HMAC-SHA-256



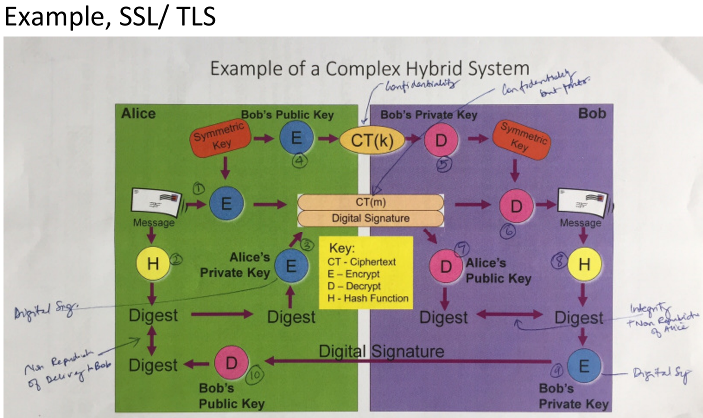
   b. CBC-MAC
4. Digital Signature – Asymmetric key used to provide sender Non-Rep
   a. RSA-MD5, RSA-SHA1, RSA-SHA-256, DSA



5. Birthday Attack. Ability to find another message that has the same hash value. Easier with smaller hash lengths. That's why SHA-256 is rising.

d. Hybrid

i. Asymmetric to generate ephemeral secret key
ii. Hash Function to ensure integrity and non-repudiation of ephemeral key
iii. Symmetric to transfer bulk content using the ephemeral key
iv. Example, SSL/ TLS



5. Summary

	Encryption	Digital Signature	Hash Function	Key Distribution
Symmetric Key Algorithms				
DES	X			
3DES	X			
AES	X			
Blowfish	X			
IDEA	X			
RC4	X			
Asymmetric Key Algorithms				
RSA	X	X		X
ECC	X	X		X
ElGamal, EC-ElGamal	X	X		X
DSA, EC-DSA		X		
Diffie-Hellman (DH), EC-DH				X
Hash Function				
RSA: MD2, MD4, MD5			X	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512			X	
HAVAL			X	

6. Attacks on Cryptography - Increasing computational power has led to successful attacks on various implementations. MD5 and SHA-1 have been broken.

Attack	Notes	PT	CT	Algo	Key	Work Factor
Ciphertext-only	Attacker has CT block(2) only. Commonly done, but very hard to crack	N	Y	N	N	Extreme
Known Plaintext	Has combo(s) of PT (or parts) and CT. In ECB case, this can lead to crack. Used in Enigma	Y	Y	N	N	High/Ext
Chosen Plaintext	Can get CT for a PT of his choice	Y	Y	Y	N	High
Chosen Ciphertext (Lunchtime)	Can get PT for a CT of his choice. Harder to do because need access to targets PC. RSA hit	Y	Y	N	N	High
Differential Cryptanalysis	Type of Chosen Plaintext, Side Channel attack – slightly different PTs are encrypted and likely keys deduced by analysis	Y	Y	Y	N	Medium
Linear Cryptanalysis	Type of Chosen Plaintext – many PTs encrypted, and key deduced by statistics	Y	Y	Y	N	Medium
Implementation Attacks	Most common – attack the implementation weaknesses, not the algo. Example side channel, Fault analysis, Probing attacks					
Frequency Attacks	For substitution ciphers – where stats of PT are known	Y				
Side Channel Attacks	Observe other factors like processing time, power, radiation, heat to infer keys	N	N	Y	N	
Replay Attack	Resends spoofed original auth request. Can be caught by timestamping and sequence checks			Y		
Algebraic, Analytic, Statistical attacks	Focus on vulnerabilities in algo instead of full key-space brute force to reduce work factor			Y		
Meet-in-the-middle attack	Encrypting at one end and decrypting at the other end					
Rainbow Table Attack	Database of hash values – providing reverse lookup		Y	Y		
Dictionary Attack	Using all possible word combinations to brute force a password					
Brute Force	Trying all possible passwords					