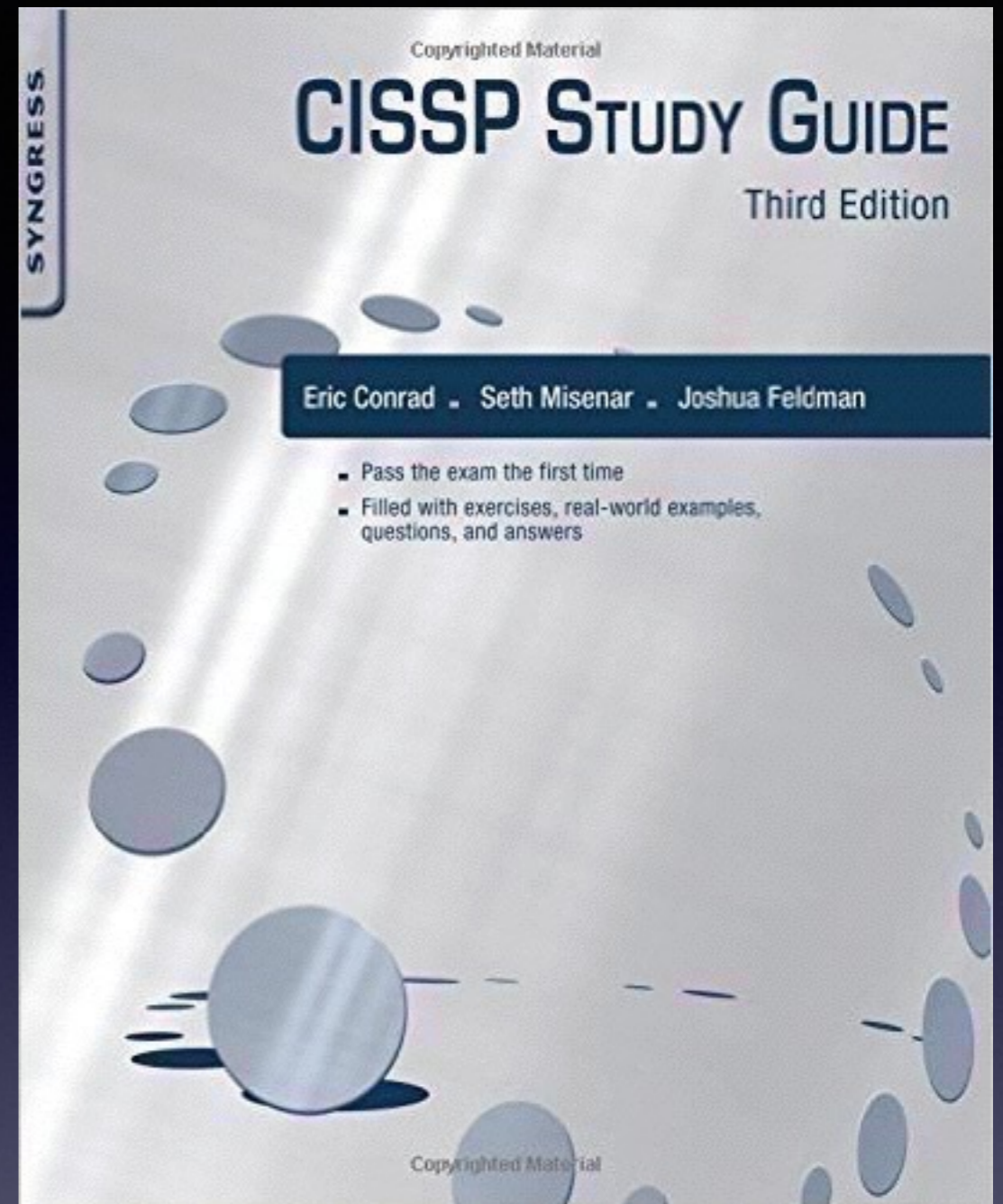


CNIT 125: Information Security Professional (CISSP Preparation)



Ch 4. Security Engineering (Part 2)

Rev. 10-27-17

Topics in Part 2

- **Cornerstone Cryptographic Concepts**
- **History of Cryptography**
- **Types of Cryptography**
- **Cryptographic Attacks**
- **Implementing Cryptography**
- **Perimeter Defenses**
- **Site Selection, Design, and Configuration**
- **Environmental Controls**

Cornerstone Cryptographic Concepts

Key Terms

- **Cryptology**
 - **The science of secure communications**
- **Cryptography**
 - **Secret writing**
- **Cryptanalysis**
 - **Breaking encrypted messages**

Key Terms

- **Cipher**
 - **A cryptographic algorithm**
- **Plaintext**
 - **An unencrypted message**
- **Encryption turns plaintext into *cipher text***
- **Decryption turns cipher text into plaintext**

Confidentiality and Integrity

- **Confidentiality**
 - **Secrets remain secret**
- **Integrity**
 - **Data is not altered by unauthorized subjects**

Authentication and Nonrepudiation

- **Authentication**
 - **Verifies the identity of a user**
- **Nonrepudiation**
 - **Assurance that audit records are accurate**
 - **So subjects cannot deny what they did later**

Confusion and Diffusion

- **Confusion**
 - **No relationship between plaintext and ciphertext**
- **Diffusion**
 - **Plaintext should be dispersed throughout the ciphertext**

Substitution and Permutation

- **Substitution**
 - **Replacing one character with another**
 - **Provides confusion**
- **Permutation**
 - **Rearranging letters**
 - **Provides diffusion**

Cryptographic Strength

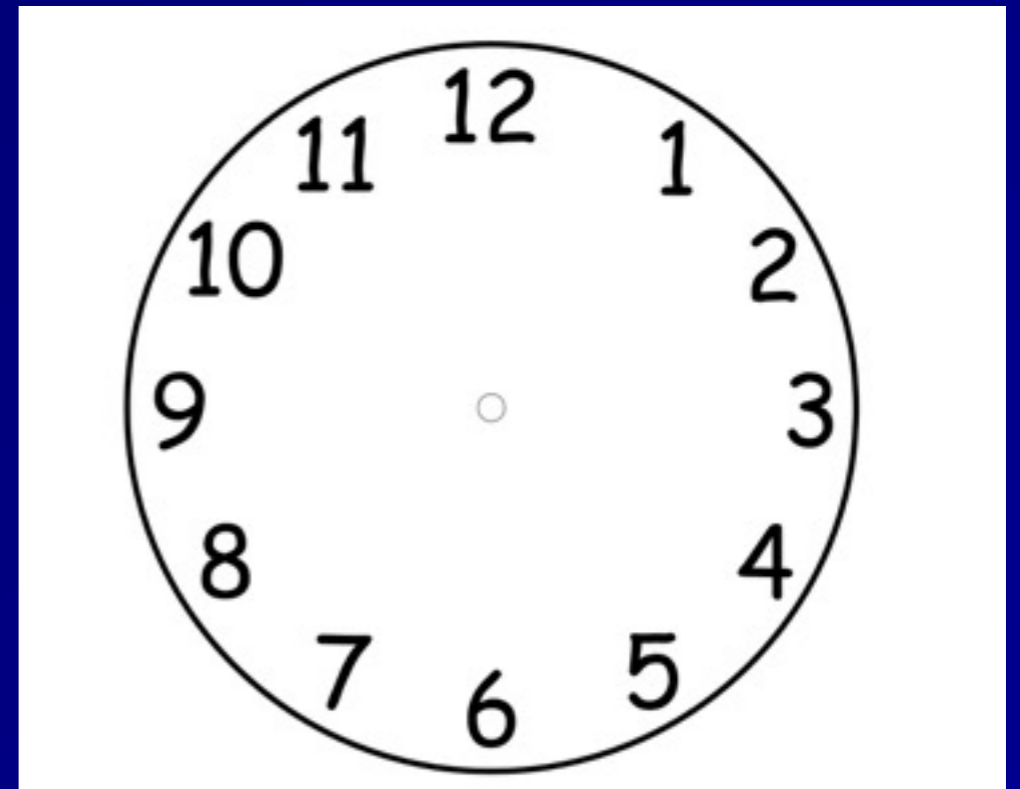
- **Strong encryption**
 - **Very difficult or impossible to decrypt without the key**
- **Work factor**
 - **How long it will take to break a cryptosystem**
- **Secrecy of the system does not provide strength**
 - **Stupid proprietary systems are weaker than well-known strong systems**

Monoalphabetic and Polyalphabetic Ciphers

- **Monoalphabetic**
 - **One plaintext letter changes to one ciphertext letter**
 - **Can be broken by *frequency analysis***
 - **Most common letter is E**
- **Polyalphabetic Ciphers**
 - **Use multiple substitutions for each letter**
 - **Resists frequency analysis**

Modular Math

- Numbers are on a ring
- The "modulus" specifies how many numbers are used
- A clock is modulus 12
 - $12 + 1 = 1 \pmod{12}$
 - $7 + 7 = 2 \pmod{12}$
 - $1 - 2 = 11 \pmod{12}$



Exclusive OR

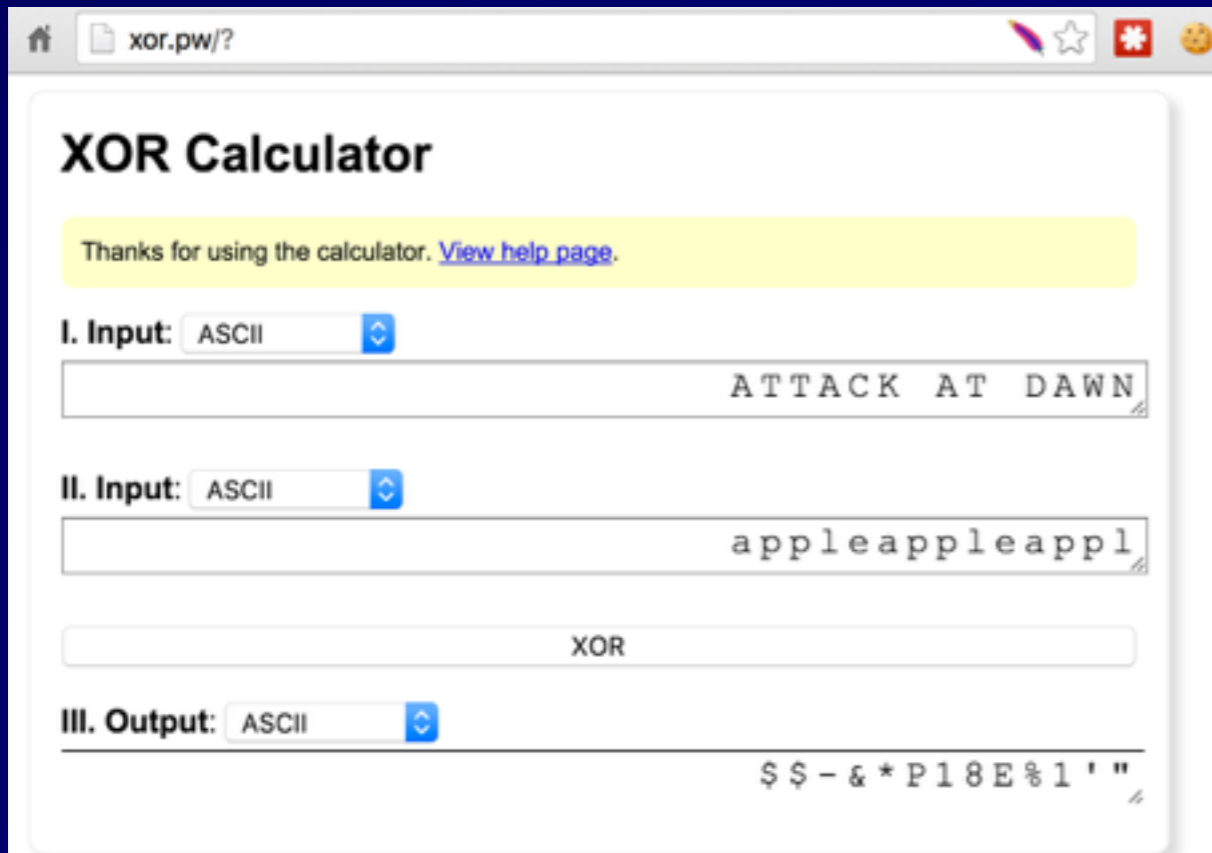
- $0 \text{ XOR } 0 = 0$
- $0 \text{ XOR } 1 = 1$
- $1 \text{ XOR } 0 = 1$
- $1 \text{ XOR } 1 = 0$

Table 4.4

01000001 XORed to 01010101

Plaintext	0	1	0	0	0	0	0	1
Key	0	1	0	1	0	1	0	1
Ciphertext	0	0	0	1	0	1	0	0

XOR Reverses Itself



xor.pw/?

XOR Calculator

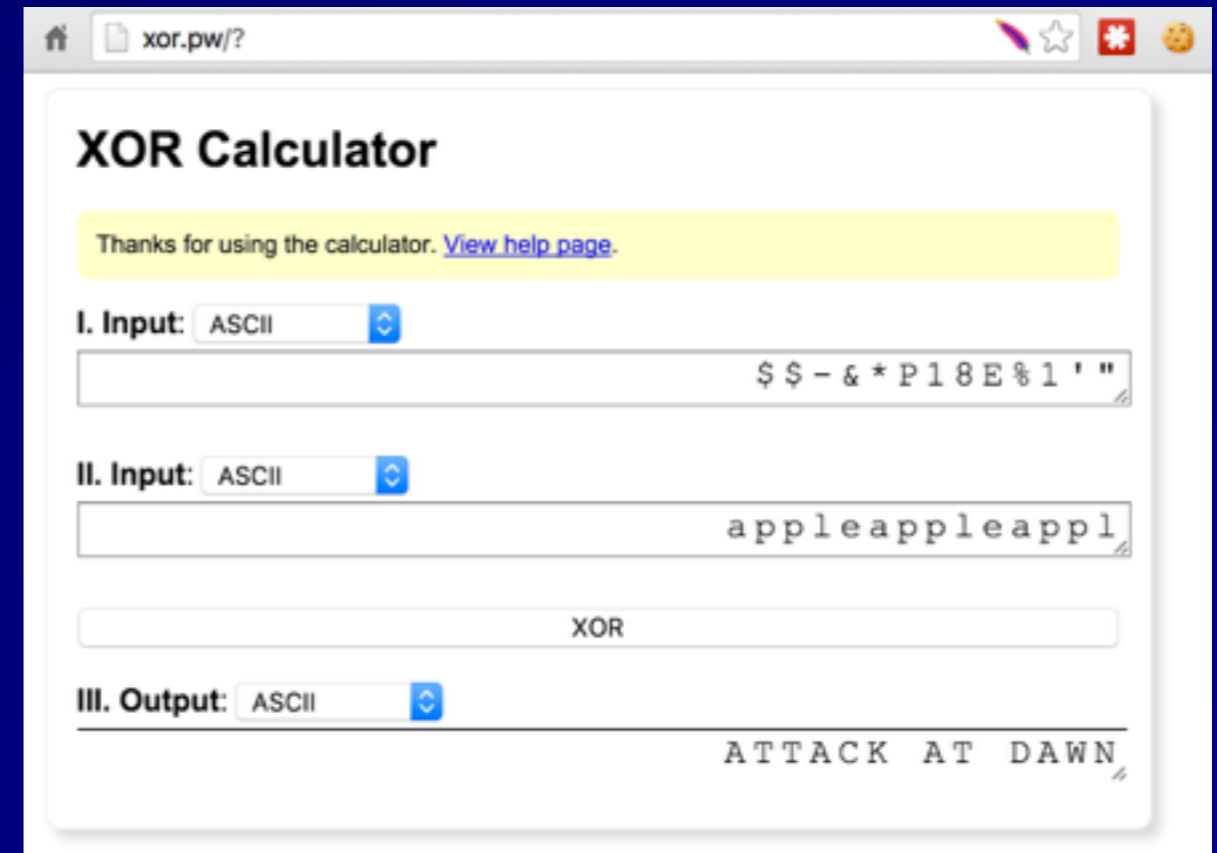
Thanks for using the calculator. [View help page.](#)

I. Input: ASCII

II. Input: ASCII

XOR

III. Output: ASCII



xor.pw/?

XOR Calculator

Thanks for using the calculator. [View help page.](#)

I. Input: ASCII

II. Input: ASCII

XOR

III. Output: ASCII

Data at Rest and Data in Motion

- **Data at Rest**
 - **Whole-disk encryption (if power is off)**
- **Data in Motion**
 - **End-to-end encryption**
 - **Attackers in the middle won't have the key**
 - **VPNs provide this protection**

Protocol Governance

- **Selecting appropriate encryption methods**
- **Must weigh considerations:**
 - **Speed**
 - **Strength**
 - **Cost**
 - **Complexity**
 - **And others**

Kahoot!

History of Cryptography

Spartan Scytale

- **Wrap parchment around a rod**
- **Letters are rearranged**
 - **Transposition**

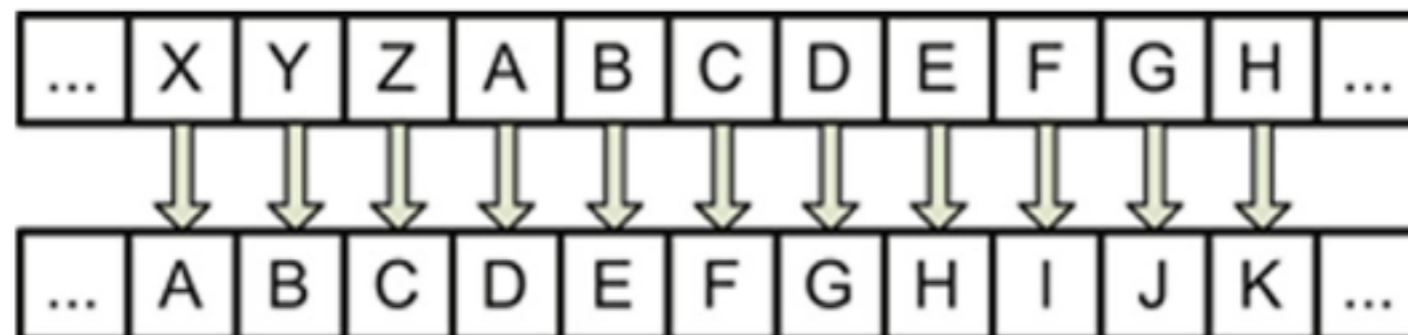


Caesar Cipher

- **Substitution cipher**
- **ROT-13 is still used by Microsoft**

Table 4.6

Caesar (Rot-3) Cipher



Vigenerere Square

Polyalphabetic Substitution Cipher

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	U	V	W	X	Y	Z	
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	V	W	X	Y	Z	A	
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B	
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

FIGURE 4.18 Vigenère Square Encrypting Plaintext "T" with a Key of "E"

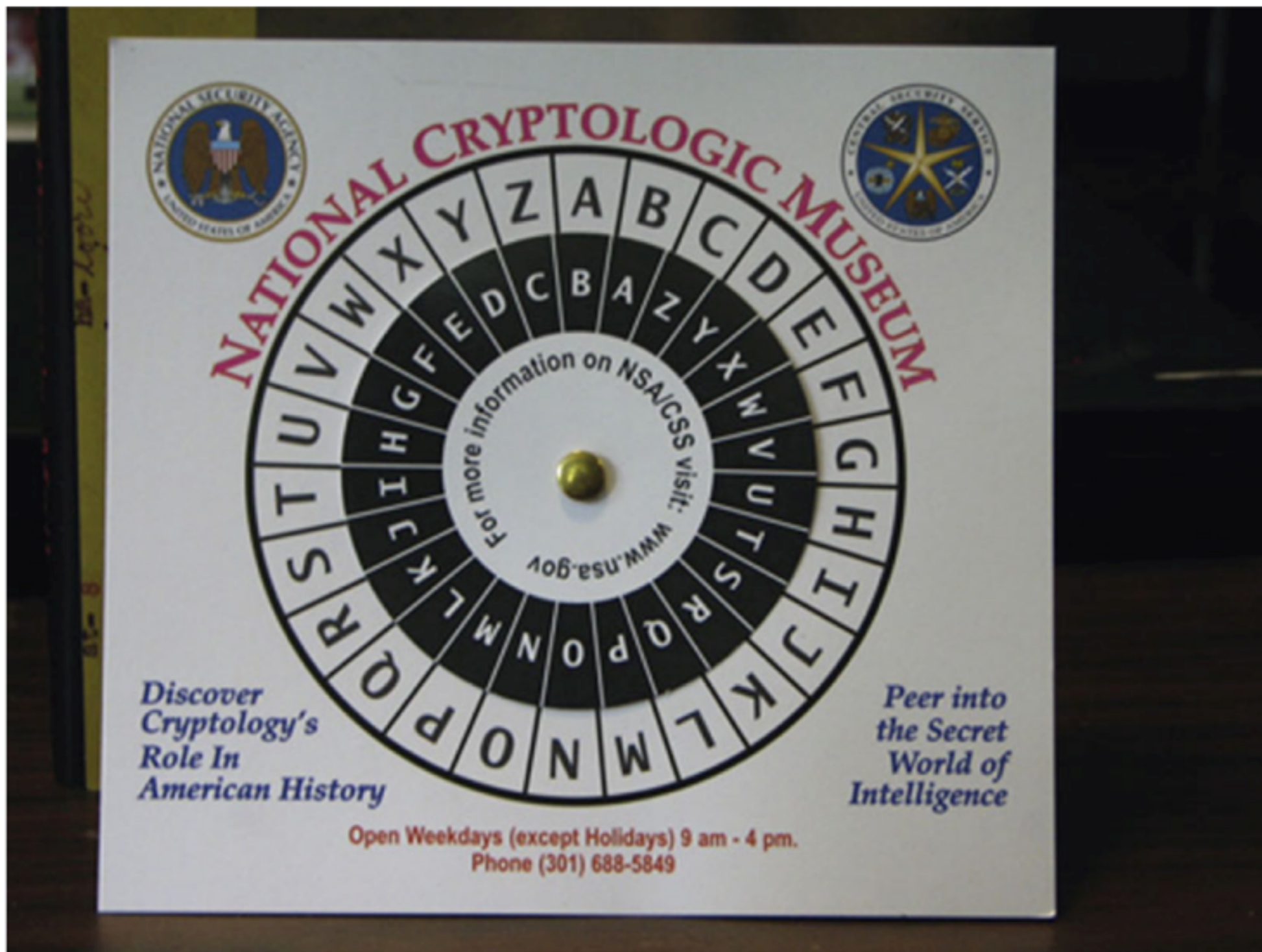


FIGURE 4.19 A Modern Cipher Disk from the National Cryptologic Museum Courtesy of the National Security Agency



FIGURE 4.20 Confederate States of America Cipher Disks

Book Cipher

- **Ciphertext is a series of numbers**
 - **158.9.25 115.9.12 ...**
 - **Page 158, paragraph 9, word 25**
 - **Page 115, paragraph 9, word 12**
- **Recipient must have the same book as sender**

Running-Key Cipher

- Agree to use a phrase or document as the key
- Such as the Constitution

Table 4.8

Running Key Ciphertext of "ATTACK AT DAWN"

A	T	T	A	C	K	A	T	D	A	W	N
+	+	+	+	+	+	+	+	+	+	+	+
W	E	T	H	E	P	E	O	P	L	E	O
=	=	=	=	=	=	=	=	=	=	=	=
X	Y	N	I	H	A	F	I	T	M	B	C

Codebooks

- **Assign code words for important people, locations, and terms**
 - **The US Secret Service uses code names for the First Family**
 - **Hillary Clinton is "Evergreen"**
 - **Barack Obama is 'Renegade"**
 - **Link Ch 4e**

One-Time Pad

- **Sender and recipient must have a pad with pages full of random letters**
- **Each page is used only once**
- **Mathematically unbreakable**
 - **The only way to break it is to steal or copy the pad**
 - **Key distribution is burdensome: distributing the pads**
- **Vernam was the first to use it, in 1917**

Project VERONA

- **KGB used one-time pads in the 1940s**
- **US and UK cryptanalysts broke it**
- **Because the KGB cheated and re-used the pads**

Hebern Machines

- **Look like large manual typewriters**
- **Encrypt and decrypt data**
- **Enigma used by the Nazis**
- **SIGBABA used by the USA into the 1950s**
- **Purple used by the Japanese in WW II**

Cryptography Laws

- **COCOM (Coordinating Committee for Multilateral Export Controls)**
 - **In effect from 1947 - 1994**
 - **Applied to US, some European countries, Japan, AU, and more**
 - **To control export to Iron Curtain countries**
- **Wassenaar Arrangement**
 - **Created in 1996**
 - **Relaxed many restrictions on cryptography**

Types of Cryptography

Three Types of Cryptography

- **Symmetric encryption**
 - **Provides confidentiality**
 - **Uses one key**
- **Asymmetric encryption**
 - **Provides confidentiality**
 - **Each user has two keys**
- **Hashing**
 - **No key at all**
 - **Provides integrity, not confidentiality**

Symmetric Encryption

- **Same key used to encrypt and decrypt**
- **Also called "secret key"**
- **Key Distribution**
 - **Secret key must be securely transmitted to recipient**

Stream and Block Ciphers

- **Stream**
 - **Encrypts one bit at a time**
 - **Ex: RC4 (used in WEP)**
- **Block**
 - **Encrypts one block of data at a time**
 - **DES used a 64-bit block size**
 - **AES uses 128-bit blocks**

Initialization Vector (IV) & Chaining

- **IV is a random value added to the plaintext before encryption**
 - **To ensure that two identical plaintext messages don't encrypt to the same ciphertext**
- **Chaining**
 - **Uses the result of one block to determine a "seed" to add to the next block**

DES (Data Encryption Standard)

- **Describes DEA (Data Encryption Algorithm)**
- **Based on IBM's Lucifer algorithm**
 - **Lucifer used a 128-bit key**
 - **DES used 56-bit key**

Modes of DES

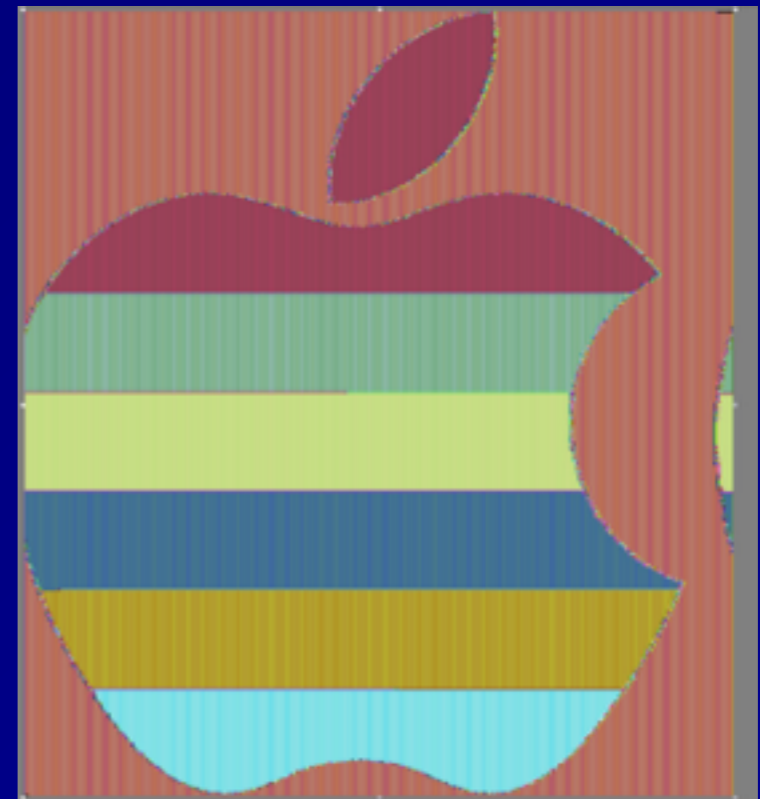
- **Electronic Code Book (ECB)**
- **Cipher Block Chaining (CBC)**
- **Cipher Feedback (CFB)**
- **Output Feedback (OFB)**
- **Counter Mode (CTR)**

Electronic Code Book (ECB)

- **Simplest and weakest form of DES**
- **No initialization vector or chaining**
- **Two messages with identical plaintexts result in identical ciphertexts**
- **Some patterns are therefore preserved in ciphertext (see next slide)**

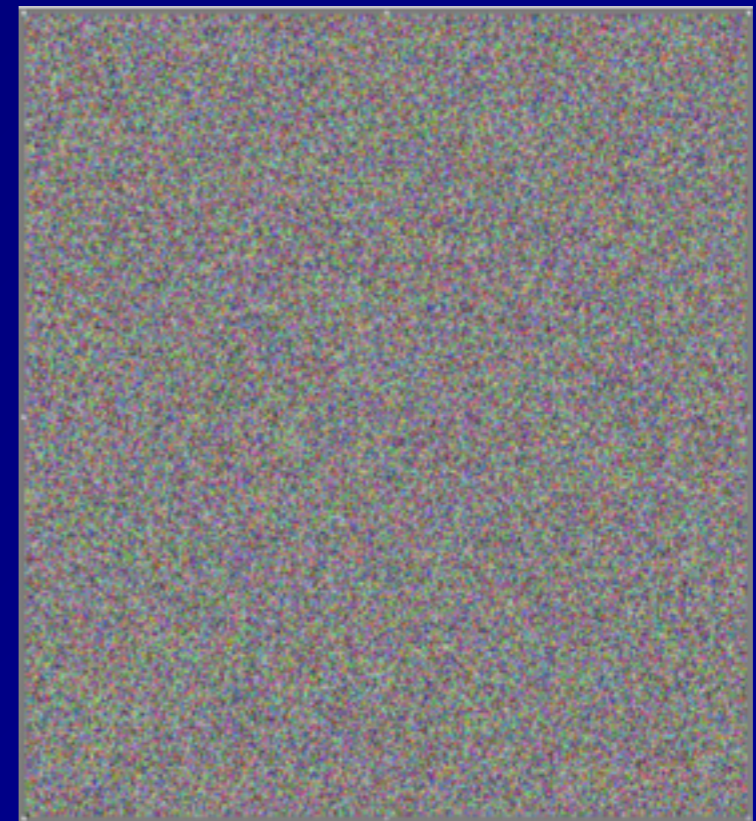
ECB Mode

- **Identical regions in original image remain identical in ciphertext**
- **Encryption is not hiding all the information in the plaintext**



CBC Mode

- All patterns are obscured
- Similar results for
 - CBC
 - CFB
 - OFB
 - CTR



Single DES

- **The original implementation of DES**
- **Uses a single 56-bit key**
- **Broken by brute force in 1997**
- **No longer considered secure**

Triple DES

- **Three rounds of DES encryption**
- **Using two or three different 56-bit keys**
- **Effective key length is 112 bits or more**
- **Considered secure, but slower to compute than AES**

International Data Encryption Algorithm

- **Symmetric block cipher**
- **International replacement for DES**
- **Patented in many countries**
- **128-bit key; 64-bit block size**
- **Considered secure**
- **Drawbacks: encumbered by patents, and slower to compute than AES**

Advanced Encryption Standard (AES)

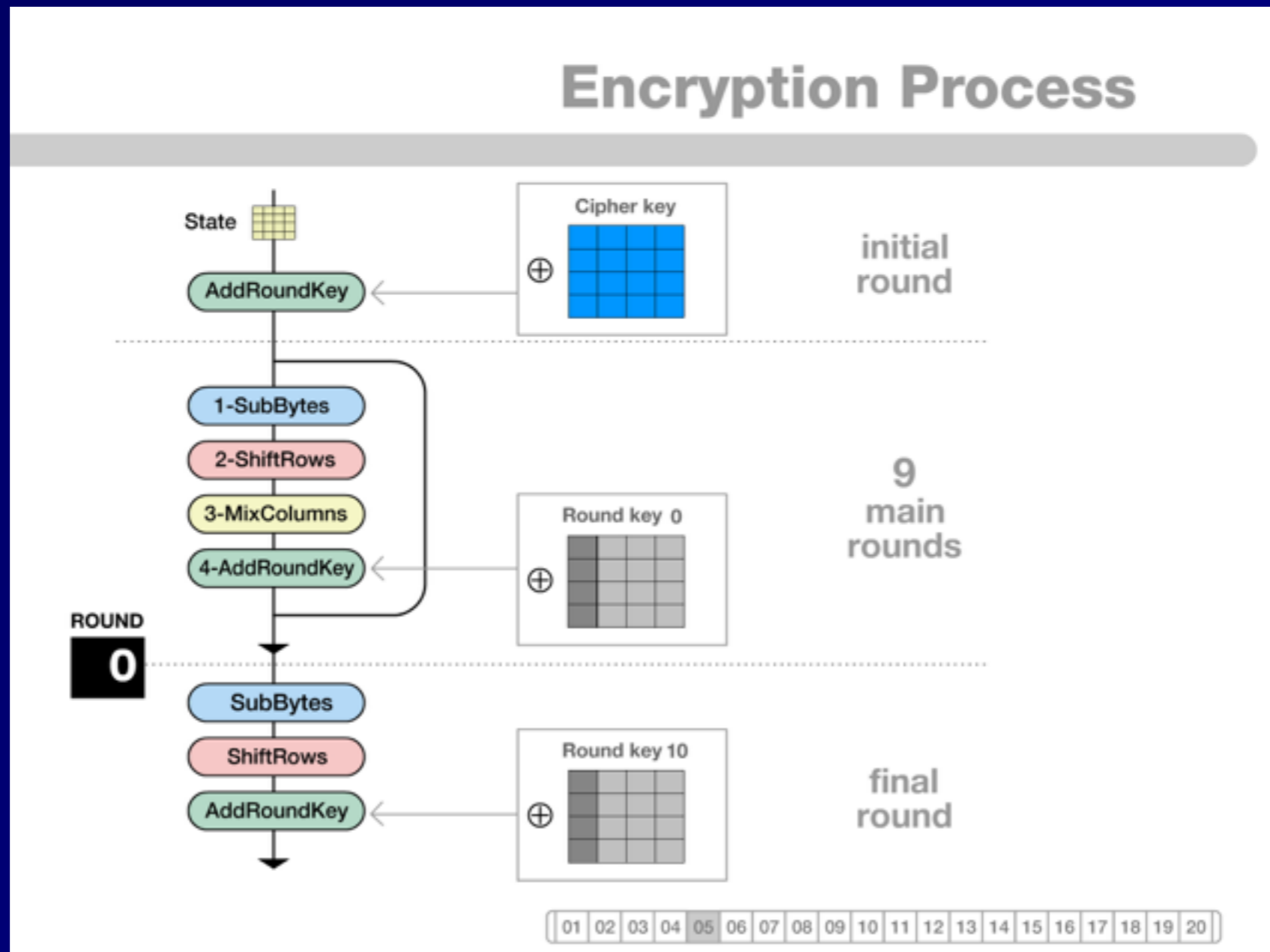
- **Current US recommended standard**
- **Three key lengths: 128, 192, and 256-bits**
- **Open algorithm, patent-free**
- **Uses the Rindjael algorithm**

Table 4.12

Five AES Finalists

Name	Author
MARS	IBM
RC6	Rivest, Robshaw, Sidney, Yin
Rijndael	Daemen, Rijmen
Serpent	Anderson, Biham, Knudsen
Twofish	Schneier, Kelsey, Hall, Ferguson, Whiting, Wagner

Pretty Rindjael Animation



- [Link Ch 4f](#)

Blowfish and Twofish

- **Symmetric block ciphers**
- **Developed by Bruce Schneider**
- **Open algorithms, unpatented, and freely available**
- **Blowfish key sizes: 32 - 448 bit**
- **Two fish key sizes: 128 - 256 bits**

RC5 and RC6

- **Block ciphers by RSA Laboratories**
- **RC5 uses 32-bit, 64-bit, or 128-bit blocks**
 - **Key size: 0 - 2040 bit**
- **RC6**
 - **Stronger than RC5**
 - **128-bit block sizes**
 - **Key sizes: 128, 192, or 256 bits**

Asymmetric Encryption

- **Based on Diffie-Hellman key exchange**
- **First form was RSA algorithm (1977)**
- **Each user makes two keys**
 - **Public key is shared with the world**
 - **Private key is kept secret**
- **Anyone can send you secrets using your public key**
- **Only you can open them, with your private key**

One-Way Functions

- **It must be way to calculate a public key from the private key**
- **But impossible to deduce the private key from the public key'**
- **Using a mathematical function that's easy to compute but hard to reverse**

One-Way Functions

- **Factoring a Large Number**
 - **Into its component primes**
 - **Used by RSA algorithm**
- **Discrete Logarithm**
 - **Used by Diffie-Hellman and ElGamal asymmetric algorithms**
- **Elliptic Curve Cryptography**
 - **Faster to compute than RSA**
 - **Popular on mobile devices**

Asymmetric v. Symmetric Encryption

- **Symmetric algorithms use shorter keys and are faster**
- **In RSA, asymmetric crypto is used to send a symmetric *session key***

Table 4.16

Symmetric vs. Asymmetric Strength [25]

Symmetric Key Length	Symmetric Algorithm	Discrete Logarithm Equivalent Key Length	Factoring Prime Numbers Equivalent Key Length	Elliptic Curve Equivalent Key Length
112	3TDES	2048	2048	224-255
128	AES	3072	3072	256-283
192	AES	7860	7860	384-511
256	AES	15360	15360	512+

Hash Functions

- **All the bytes in an input file are combined to form a fixed-length "hash" or "fingerprint"**
- **MD5: 128 bits long (insecure)**
- **SHA-1: 160 bits (No longer trusted)**
- **SHA-2: 224 bits or longer (secure)**
- **SHA-3: too new for the CISSP exam**
- **HAVAL (Hash of Variable Length)**
 - **128 bits or longer**

Collisions

- **A hash should be unique in practice**
- **No two different files should have the same hash (a "collision")**
- **MD5 has known collisions**
- **SHA-1 collisions are expected to be found this year (2016)**
- **Everyone is moving to SHA-2 now**

Kahoot!

Cryptographic Attacks

Brute Force

- **Try every possible key**
- **In principle, will always work**
 - **Except against the one-time pad**
- **Impossible in practice if key is long enough**
 - **128 bits for a symmetric key**
 - **2048 bits for an RSA key**

Social Engineering

- **Trick subject into revealing the key**

Rainbow Tables

- **Pre-computed table of passwords and hashes**
- **Time-memory tradeoff**
- **Not very practical for modern hash algorithms**
- **Very effective against Windows XP's LANMAN hashes**

Known Plaintext

- **If plaintext is known or can be guessed, some mathematical attacks get easier**
- **Some WEP cracks use this message**
 - **Portions of ARP packets can be guessed**

Chosen Plaintext Attack

- **Choosing plaintext that must be padded to fill the block size**
- **Can reveal information about the key**
- **"Padding Oracle" attacks**
 - **BEAST, CRIME, other attacks**

Meet-in-the-Middle Attack

- **Do half the encryption steps from plaintext**
- **Do half the decryption steps from the ciphertext**
- **Can make the calculation MUCH faster**
 - **Effectively halving the key size**
- **This is why people use 3DES, not 2DES**

Known Key

- **Attacker may have some knowledge about the key**
- **Ex: key is based on a dictionary word, or contains only uppercase characters**

Differential Cryptanalysis

- **Encrypt two plaintexts that differ by only a few bits**
- **Statistical analysis of ciphertext reveals information about the key**

Side-Channel Attacks

- **Monitor some physical data that reveals information about the key**
 - **Timing of calculation**
 - **Power consumption**

Implementation Attacks

- **Exploit a vulnerability in the actual system used to perform the math**
- **System may leave plaintext in RAM or temporary files**
- **Key may be left on the hard drive**

Birthday Attack

- A room with 23 people has $23 \times 22 / 2$ *pairs* of people
- So there are usually two people with the same birthday
- Hash collisions are found at half the hash size
- MD5 (128 bits) will have a collision after 2^{64} calculations

Implementing Cryptography

Digital Signatures

- Calculate hash of document
- Encrypt it with your private key
- Anyone can verify it with your public key
- Provides authentication, integrity, and nonrepudiation, but not confidentiality



FIGURE 4.30 Creating a Digital Signature [\[30\]](#)

Verifying a Digital Signature

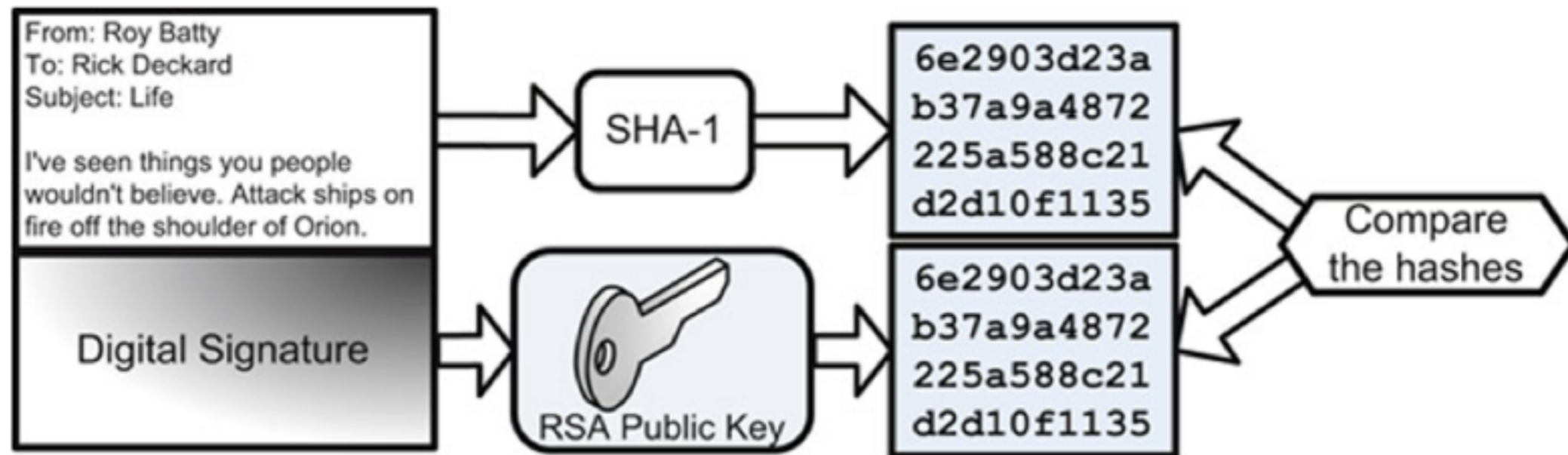


FIGURE 4.31 Verifying a Digital Signature

Message Authentication Code (MAC)

- **Verifies authenticity of a message using hashing and a shared secret key**
- **Provides integrity and authenticity**
 - **CBC-MAC uses CBC mode of DES**

HMAC

- **Hashed Message Authentication Code**
- **A type of MAC**
- **Uses a shared secret and a hashing algorithm**
 - **HMAC-MD5**
 - **HMAC-SHA-1**

Public Key Infrastructure (PKI)

- **Manages *digital certificates***
- **A public key signed with a digital signature**
- **Server-based**
 - **On an HTTPS server**
- **Client-based**
 - **Bound to a person**
- **Mutual authentication**
 - **Authenticates server and client**

Five Components of PKI

- **Certificate Authorities**
 - **Issue and revoke certificates**
- **Organizational Registration Authorities**
 - **Authenticate users and issue certificates to them**
- **Certificate holders (can sign documents)**
- **Clients that validate signatures**
- **Repositories that hold certificates and Certificate Revocation Lists**
 - **Online Certificate Status Protocol is a newer system to replace CRLs**

Key Management Issues

- **Private keys must be protected, like passwords**
- **Backing up a private key may use *key escrow***
- **Copy of a key (or part of a key) held by a trusted third party**

SSL & TLS

- **Secure Sockets Layer was the first system**
- **Now replaced by Transaction Layer Security**

SSL Handshake

Source	Destination	Protocol	Length	Info
192.168.1.109	23.205.69.135	TCP	78	61048 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=2267861530 TSecr=...
23.205.69.135	192.168.1.109	TCP	74	443 → 61048 [SYN, ACK] Seq=0 Ack=1 Win=28240 Len=0 MSS=1424 SACK_PERM=1 TSval=...
192.168.1.109	23.205.69.135	TCP	66	61048 → 443 [ACK] Seq=1 Ack=1 Win=131296 Len=0 TSval=2267861759 TSecr=12616314...
192.168.1.109	23.205.69.135	TLSv1.2	269	Client Hello
23.205.69.135	192.168.1.109	TCP	66	443 → 61048 [ACK] Seq=1 Ack=204 Win=29312 Len=0 TSval=1261631650 TSecr=2267861...
23.205.69.135	192.168.1.109	TLSv1.2	1514	Server Hello
23.205.69.135	192.168.1.109	TCP	1514	[TCP segment of a reassembled PDU]
192.168.1.109	23.205.69.135	TCP	66	61048 → 443 [ACK] Seq=204 Ack=2897 Win=128416 Len=0 TSval=2267861985 TSecr=126...
23.205.69.135	192.168.1.109	TCP	1266	[TCP segment of a reassembled PDU]
192.168.1.109	23.205.69.135	TCP	66	61048 → 443 [ACK] Seq=204 Ack=4097 Win=129856 Len=0 TSval=2267861986 TSecr=126...
23.205.69.135	192.168.1.109	TLSv1.2	579	Certificate
192.168.1.109	23.205.69.135	TCP	66	61048 → 443 [ACK] Seq=204 Ack=4610 Win=130528 Len=0 TSval=2267861986 TSecr=126...
192.168.1.109	23.205.69.135	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
23.205.69.135	192.168.1.109	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
192.168.1.109	23.205.69.135	TCP	66	61048 → 443 [ACK] Seq=330 Ack=4852 Win=130816 Len=0 TSval=2267862239 TSecr=126...
192.168.1.109	23.205.69.135	TLSv1.2	475	Application Data

IPSec

- **Two primary protocols**
 - **Authentication Header (AH)**
 - **Encapsulating Security Payload (ESP)**
- **Supporting protocols**
 - **Internet Security Association and Key Management Protocol (ISAKMP)**
 - **Internet Key Exchange (IKE)**

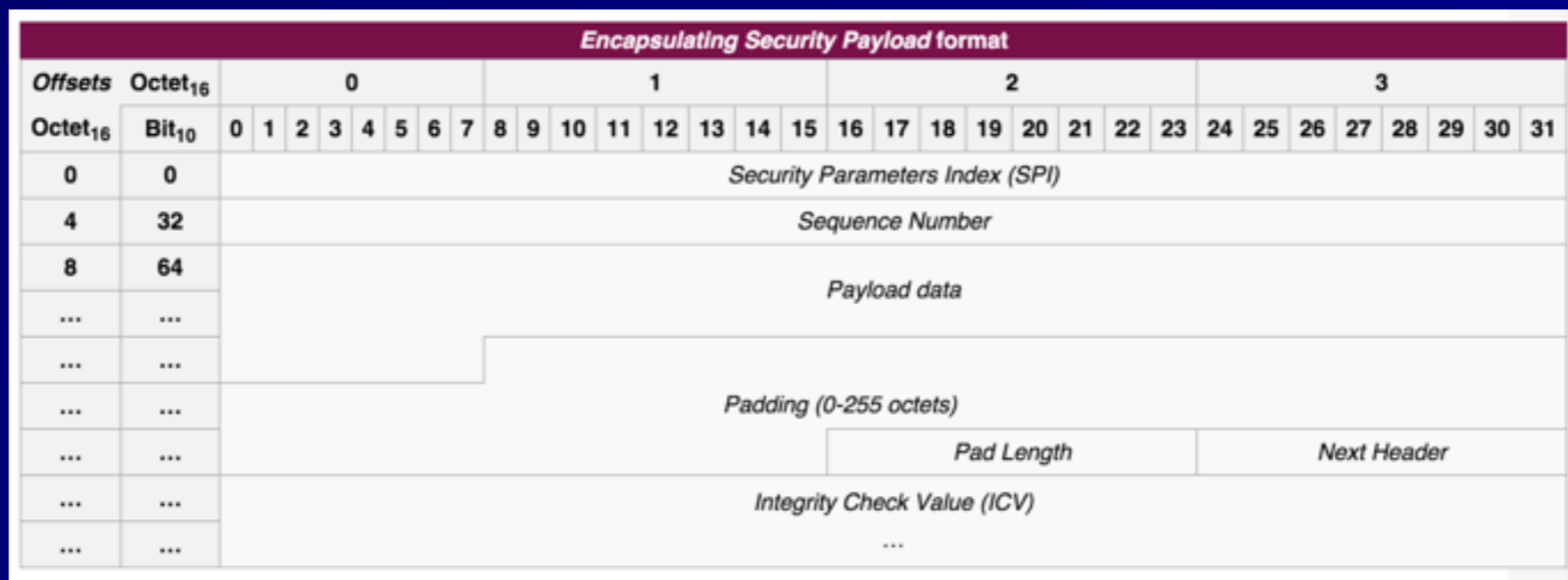
Authentication Header (AH)

- Provides authentication and integrity for each packet
- No confidentiality
- Acts as a digital signature for data
- Prevents *replay attacks*

Authentication Header format																																	
Offsets	Octet ₁₆	0								1								2								3							
Octet ₁₆	Bit ₁₀	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Next Header								Payload Len								Reserved															
4	32	Security Parameters Index (SPI)																															
8	64	Sequence Number																															
C	96	Integrity Check Value (ICV)																															
...																															

Encapsulating Security Payload (ESP)

- **Encrypts packet data**
- **Provides confidentiality**
- **Optionally also provides authentication and integrity**



Security Association (SA)

- **A one-way connection**
- **May be used to negotiate ESP and/or AH parameters**
- **If using ESP only, two SAs required**
 - **One for each direction**
- **If using AH and ES, four SAs are required**

Internet Security Association and Key Management Protocol (ISAKMP)

- **Manages the SA creation process**
- **Security Parameter Index (SPI)**
 - **32-bit identifier for a SA**

Tunnel and Transport Mode

- **Tunnel Mode**
 - **Used by security gateways**
 - **Which provide point-to-point IPSec tunnels**
- **ESP Tunnel Mode encrypts the entire packet, including headers**
- **ESP Transport Mode encrypts data, but not headers**

Internet Key Exchange (IKE)

- **Can use a variety of algorithms**
 - **MD5 or SHA-1 for integrity**
 - **3DES or AES for confidentiality**

Pretty Good Privacy (PGP)

- **Asymmetric encryption for everyone**
 - **Posted to Usenet in 1991 by Phil Zimmerman**
 - **Serious legal threats until prosecutors dropped the case in 1996**
- **Uses *Web of Trust* instead of CAs**
 - **Users vouch for other users**
 - **"Friend of a friend"**

S/MIME

- **MIME (Multipurpose Internet Mail Extensions)**
 - **Allows attachments and foreign character sets in email**
- **S/MIME (Secure MIME)**
 - **Uses PKI to encrypt and authenticate MIME-encoded email**

Escrowed Encryption

- **Third-party organization holds a copy of a public/private key pair**
 - **Private key can be broken into two or more parts**
 - **And held by different escrow agencies**
 - **This provides separation of duties**
- **This can allow law enforcement some access to the key, while preserving some privacy**

Clipper Chip

- **Technology used in Escrowed Encryption Standard (EES)**
 - **Announced by US Gov't in 1993**
 - **For telecommunication devices**
 - **Controversial, abandoned in 1996**
- **Used Skipjack symmetric cipher**
 - **80-bit keys, secret algorithm**

Steganography

- **Hiding data inside a file**
- **The existence of the message is secret**
- **Digital Watermarks**
 - **Encode a fingerprint into a file to identify the owner**
 - **Can be used to prosecute copyright violators**

Kahoot!

Perimeter Defenses

Fences

- **3 foot**
 - **A deterrent**
- **8 foot with barbed wire on top**
 - **Preventive**

Gates

- **Ornamental (Class I)**
- **Deterrent**
- **Crash Gate (Class IV)**
- **Stops a car**

Table 4.17

Types of Vehicle Gates

Type	Description
Class I	Residential (home use)
Class II	Commercial/General Access (parking garage)
Class III	Industrial/Limited Access (loading dock for 18-wheeler trucks)
Class IV	Restricted Access (airport or prison)

Bollards

- Posts designed to stop a car



FIGURE 4.33 Stainless Steel Traffic Bollards Source:

http://commons.wikimedia.org/wiki/File:Stainless_steel_bollard_SSP150.JPG.

Photograph by Leda Vannaclip. Image under permission of Creative Commons

Attribution ShareAlike 3.0.

Lights

- **Can be detective or deterrent**
- **Rated in *lumens***

CCTV

- **Closed Circuit Television**
 - **Detective control**
 - **Infrared cameras can see in the dark**
 - **Old "tube cameras" were analog**
 - **Modern CCD (Charged Couple Discharge) cameras are digital**
- **Issues**
 - **Depth of field, field of view, pan and tilt**

Locks

- **Key locks**
 - **Code is sometimes printed on the key**
 - **Can be deduced from a photo of the key**

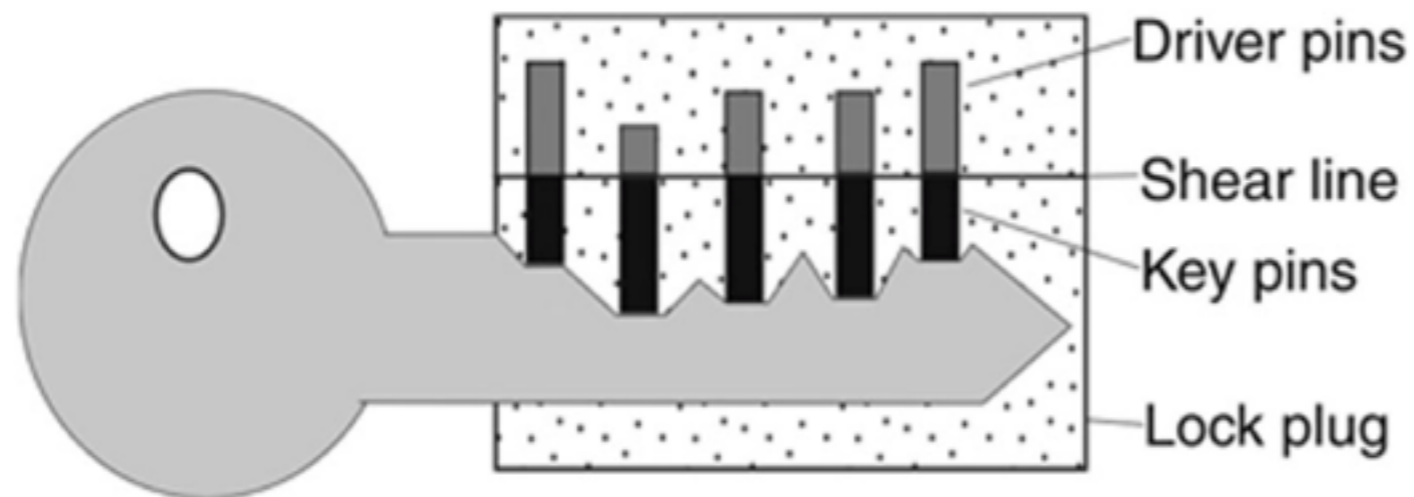


FIGURE 4.37 The Correct Key in a Pin Tumbler Lock

Lock picking

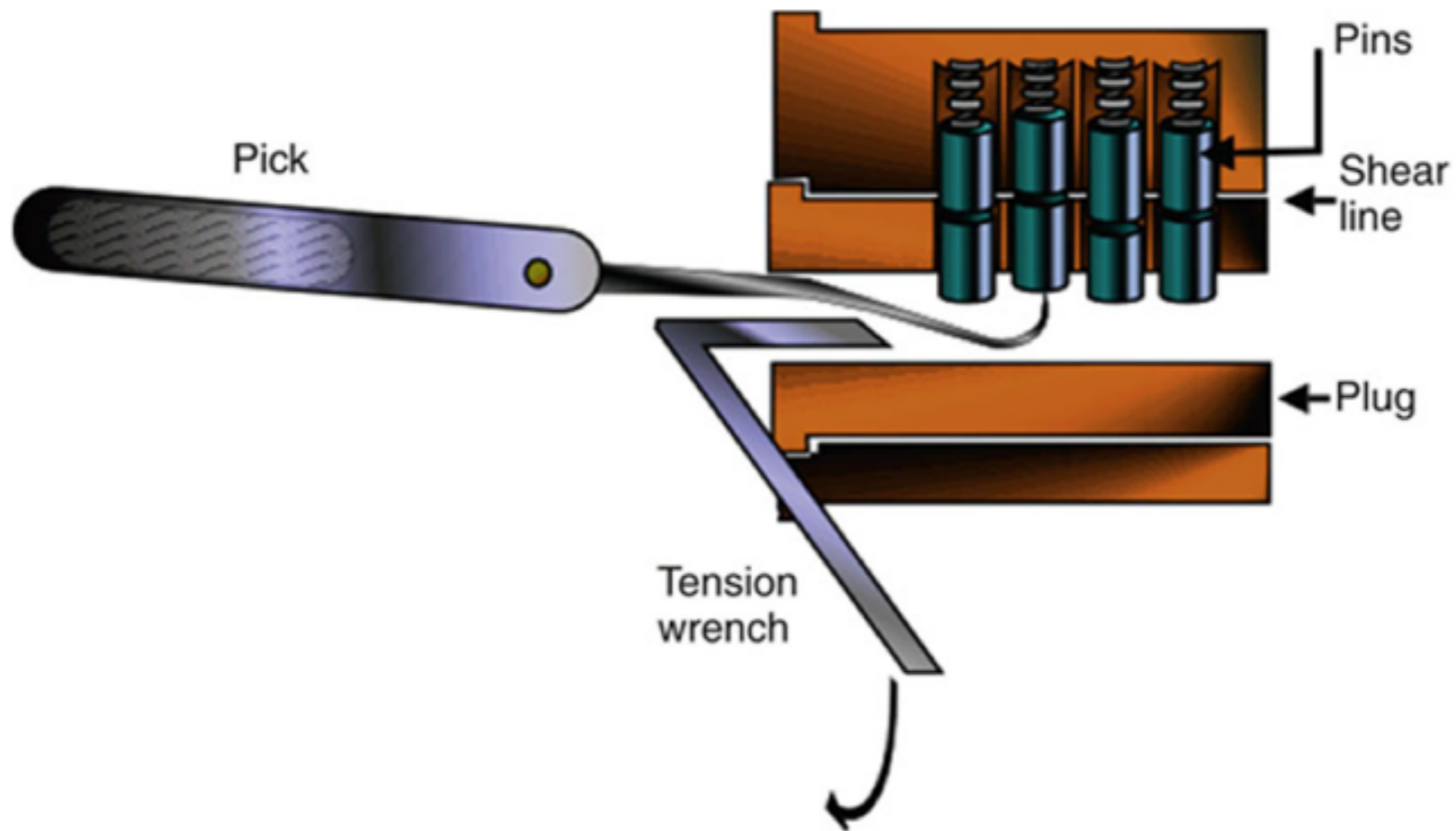


FIGURE 4.40 Picking a Pin-Tumbler Lock Source:

http://commons.wikimedia.org/wiki/File:Pin_and_tumbler_lock_picking.PNG. Drawn

Bump Keys

- **Key is shaved down to the lowest position**
- **Key is bumped to move the pins**

Master and Core Keys

- **Master key**
 - **Opens all locks in a security zone**
- **Core key**
 - **Removes the lock core**
 - **In interchangeable core locks**

Combination Locks

- **Weak control**
- **Button or keypad locks are also weak**
 - **Because, over time, the key wear down, revealing the most-used keys**
- **Vulnerable to brute-force and shoulder-surfing attacks**



Smart Cards and Magnetic Stripe Cards

- **Smart Card**
 - **Contains a computer chip**
 - **Also called "Integrated Circuit Card (ICC)"**
 - **May be "Contact" or "Contactless"**
 - **Radio-Frequency Identification (RFID) card is contactless**
- **Magstripe Card**
 - **Has data stored on a stripe of magnetic material**



FIGURE 4.41 A US Department of Defense CAC Smart Card [34]

Tailgating or Piggybacking

- **Following a person through a secure door**
- **Countermeasures**
 - **Policy forbidding it**
 - **Security awareness training**
 - **Mantraps**
 - **Chamber with two doors**
 - **Intruders are trapped inside**
 - **Turnstiles**
 - **Must allow safe egress in emergencies**

Contraband Checks

- **Identify forbidden objects**
 - **Such as weapons**
 - **Very hard to detect small storage devices like SD cards**

Motion Detectors

- **Ultrasonic and Microwave Motion Detectors**
 - **Work like Doppler Radar**
 - **Send out a signal, measure the reflected signals**
- **Photoelectric motion sensor**
 - **Sends a beam across a monitored space**
 - **Detects when the beam is broken**

Other Perimeter Alarms

- **Magnetic door and window alarms**
 - **Circuit breaks when door or window is opened**

Doors

- **Hinges should face inward**
 - **Or be otherwise protected**
- **Motion sensors can be triggered by inserting objects under the door or through gaps**
 - **Or shaking the door violently**
 - **That can trigger the emergency egress system , causing the door to open**

Windows

- **Glass is weak**
 - **Easily shattered**
- **Bulletproof glass**
- **Wire mesh or security film**
- **Lexan or Plexiglas windows**
 - **Stronger, shatter-resistant**
 - **Used in racecars and airplanes**

Walls, Floors, and Ceilings

- **Walls should go "slab to slab"**
 - **No gaps at bottom or top**
 - **Railed floors and drop ceilings can obscure where the walls stop**
- **Sheetrock can easily be cut**
- **Walls need appropriate fire rating**

Guards

- **Professional guards**
 - **Advanced training**
- **Amateur guards**
 - **"Mall cops"**
- **Orders should be complete and clear**
- **Often attacked via social engineering**

Dogs

- **Deterrent and detective controls**
- **Legal liability**
 - **Sometimes people panic and run**
 - **Dogs can kill them**

Restricted Work Areas and Escorts

- **Visitor badges can be saved and re-used**
 - **Countermeasure: time-based visitor badge control**
 - **Electronic badges that expire**
 - **Printed time and date on badge**
 - **Different badge color for each weekday**

Kahoot!

Site Selection, Design, and Configuration

Topography

- **Hills, valley, trees, etc.**
- **Can be altered with landscaping**
- **Utility Reliability and Crime**
- **Depend on the location**

Site Design and Configuration Issues

- **Site Marking**
 - **Data centers are not externally marked**
- **Shared Tenancy and Adjacent Buildings**
 - **Their poor security measures may weaken yours**
 - **Wireless networks may overlap**

Wiring Closets

- **Must be physically secured**
- **Shared Demarc**
 - **Where ISP's responsibility ends**
 - **Shared by all tenants in the building**
- **Server Rooms**
 - **Require physical access control**
 - **Also environmental controls**

Media Storage Facilities

- **Offline storage**
 - **For backup or disaster recovery**
 - **Or legal proceedings**
 - **Or regulatory compliance**
- **Must be protected from unauthorized access**
- **Some environmental controls may be needed**

System Defenses

One of the Last Lines of Defense

- **In a defense-in-depth strategy**
- **An attacker has physical access to a device or media with sensitive information**
- **Asset Tracking**
 - **Use serial #s to identify devices**
- **Port Controls**
 - **Restrict USB ports, physically or logically**

Environmental Controls

Electrical Faults

- Blackout: prolonged loss of power
- Brownout: prolonged low voltage
- Fault: short loss of power
- Surge: prolonged high voltage
- Spike: temporary high voltage
- Sag: temporary low voltage

Surge Protectors, UPSs, & Generators

- **Surge Protector**
 - **Stop voltage spikes**
- **Uninterruptible Power Supplies (UPSs)**
 - **Provide temporary power during an outage**
 - **May also clean spikes from power lines**
- **Generators**
 - **Provide power for long outages**
 - **Require fuel storage**

EMI (Electromagnetic Interference)

- **Crosstalk**
 - **Signals from one wire entering another**
- **Unshielded Twisted Pair (UTP) cable is most susceptible to EMI**
- **Shielded Twisted Pair (STP) or coaxial cable is less susceptible to EMI**
- **Fiber optic cable is immune to EMI**

HVAC (Heating, Ventilation, and Air Conditioning)

- **Positive Pressure and Drains**
 - **Air and water should be expelled from the building**
- **Data center**
 - **Humidity should be 40-55%**
 - **Temperature should be 68-77°F**

Static and Corrosion

- **Static electricity**
 - **Builds up if humidity is low**
 - **Countermeasures**
 - **Ground circuits**
 - **Antistatic wrist straps**
- **Corrosion**
 - **Caused by high humidity**

Airborne Contaminants

- **Dust can cause overheating and static buildup, or impede fans**
- **Other contaminants can cause corrosion**

Heat, Flame and Smoke Detectors

- **Heat detectors are thermometers**
- **Smoke detectors**
 - **Use *ionization* or *photoelectric* detection**
- **Flame detectors**
 - **Detect infrared or ultraviolet light**
 - **Requires line-of-sight**

Personnel Safety, Training and Awareness

- **Evacuation routes**
- **Evacuation Roles and Procedures**
 - ***Safety warden* ensures that all personnel safely leave the building**
 - ***Meeting point leader* ensures that all personnel are accounted for**
- **Handicapped people require special care**
- **Don't use elevators**

Duress Warning Systems

- **Emergency warning systems**
 - **Severe weather**
 - **Threat of violence**
 - **Chemical contamination**

ABCD Fires











CLASS OF FIRE	TYPES OF FIRE	EXTINGUISHER SYMBOLS	
		RATING SYMBOL	PICTURE SYMBOL
A Ordinary Combustibles	Wood Paper Rubber Plastic		
B Flammable Liquids	Liquids Greases Gases		
C Electrical Equipment	Energized Electrical Equipment		
D Combustible Metals	Magnesium Zinc Calcium Titanium Lithium		
K Cooking Media	Vegetable Oils Animal Oils Fats / Lards		

FIGURE 4.42 United States Fire Classes [38]

Fire Suppression Agents

- **Four methods**
 - **Reduce the temperature**
 - **Reduce supply of oxygen**
 - **Reduce supply of fuel**
 - **Interfere with chemical reaction of fire**

Fire Suppression Agents

- **Water**
 - **Good for paper or wood**
 - **Cut power before using water on electrical circuits (electrocution risk)**
- **Soda Acid**
- **Dry powder**
 - **For flammable metal fires**
- **Wet chemical**
 - **For kitchen fires**

Fire Suppression Agents

- **CO2**
 - **Dangerous; can suffocate people**
- **Halon and Halon Substitutes**
 - **Suppresses fire without suffocating people**
 - **Halon depletes the ozone, so now systems use argon, FM-200, FE-13, or Inergen**

Count-Down Timer

- **Audible and visible countdown before deploying CO2, Halon, or Halon substitutes**
- **Allows personnel to evacuate**
- **Also allows personnel to stop the release in case of a false alarm**

Sprinkler Systems

- **Wet pipe**
 - **When heat opens the sprinkler head, water flows**
- **Dry pipe**
 - **Filled with compressed air**
 - **Used in cold places where water may freeze**
- **Deluge**
 - **Large flow of water when valve opens**
- **Pre-Action**
 - **Require two triggers: fire alarm and heat at sprinkler head**
 - **Used in museums to prevent accidental discharge**

Kahoot!