This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

2021 CISSP MENTOR PROGRAM

Class 5 – April 28, 2021

Instructor:

- Brad Nigh, FRSecure – Principal Security Consultant

CISSP® MENTOR PROGRAM – SESSION FIVE

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.

FRSECURE CISSP MENTOR PROGRAM ONLINE STUDY GROUP

If you haven't done so already, and you'd like to participate, go here to register:

https://groups.io/g/FRSecure2021CISSPMentorProgram

CISSP® MENTOR PROGRAM – SESSION FIVE

KILLIN' IT!

Hope you enjoyed your break! If we overwhelm today, we have a weekend to cope.

We're through Chapters 1, 2, 3, and mostly through Chapter 4!

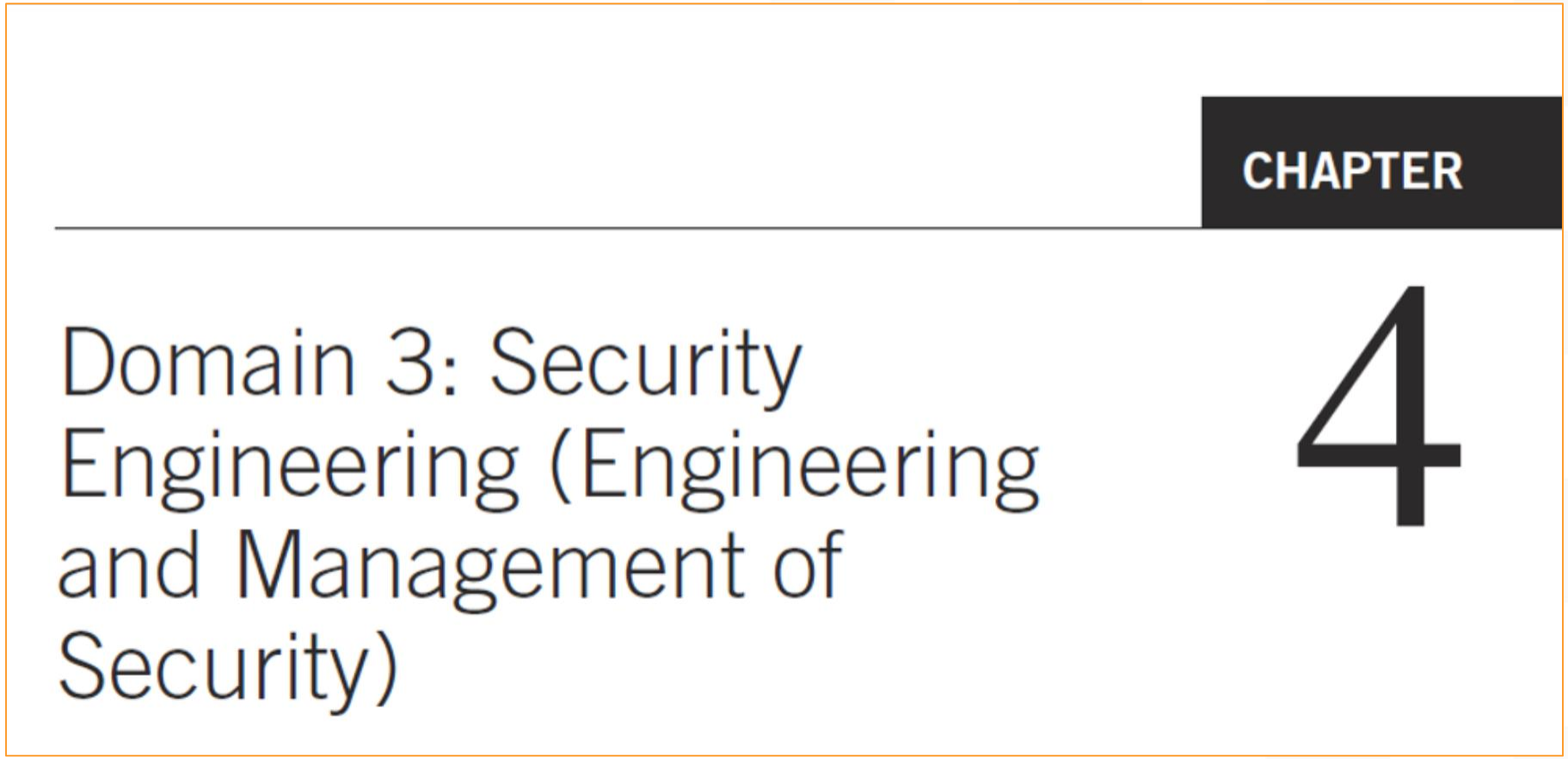
- Check-in.
- How many have read Chapter 1, 2 & 3 (and maybe 4)?
- You had some time to catch-up, but if you're in MN, you might have been distracted by sun. **Sun = Life (not testable)**
- Questions?

We're going to go fast tonight. We've got 166 slides!

CISSP® MENTOR PROGRAM – SESSION FIVE

LET'S DO THIS!

Picking up where we left off.



CISSP® MENTOR PROGRAM – SESSION FIVE

WHAT ARE WE GOING TO COVER?

Agenda – Domain 3: Security Engineering

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

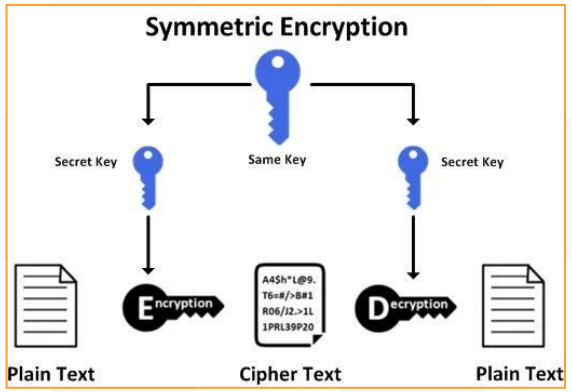
Starting on page 160 this evening

Formerly separate domains: Security Architecture, **Cryptography**, and **Physical Security**

This is the last class for this domain! Then you breathe.

LECTURE

Symmetric Encryption



- Uses **one key** to encrypt and decrypt
- Also called "**Secret key**" encryption
- Strengths include **speed** and cryptographic **strength** per bit of key
- Major weakness is that the **key must be securely shared** before two parties may communicate securely
- Keys are often shared via an out-of-band method

Stream and Block Ciphers

- Stream mode means each bit is independently encrypted in a "stream."
- Block mode ciphers encrypt blocks of data each round:
  - 56 bits for the Data Encryption Standard (DES)
  - 128, 192, or 256 bits for AES
- Some block ciphers can emulate stream ciphers by setting the block size to 1 bit; they are still considered block ciphers.

LECTURE

Symmetric Encryption

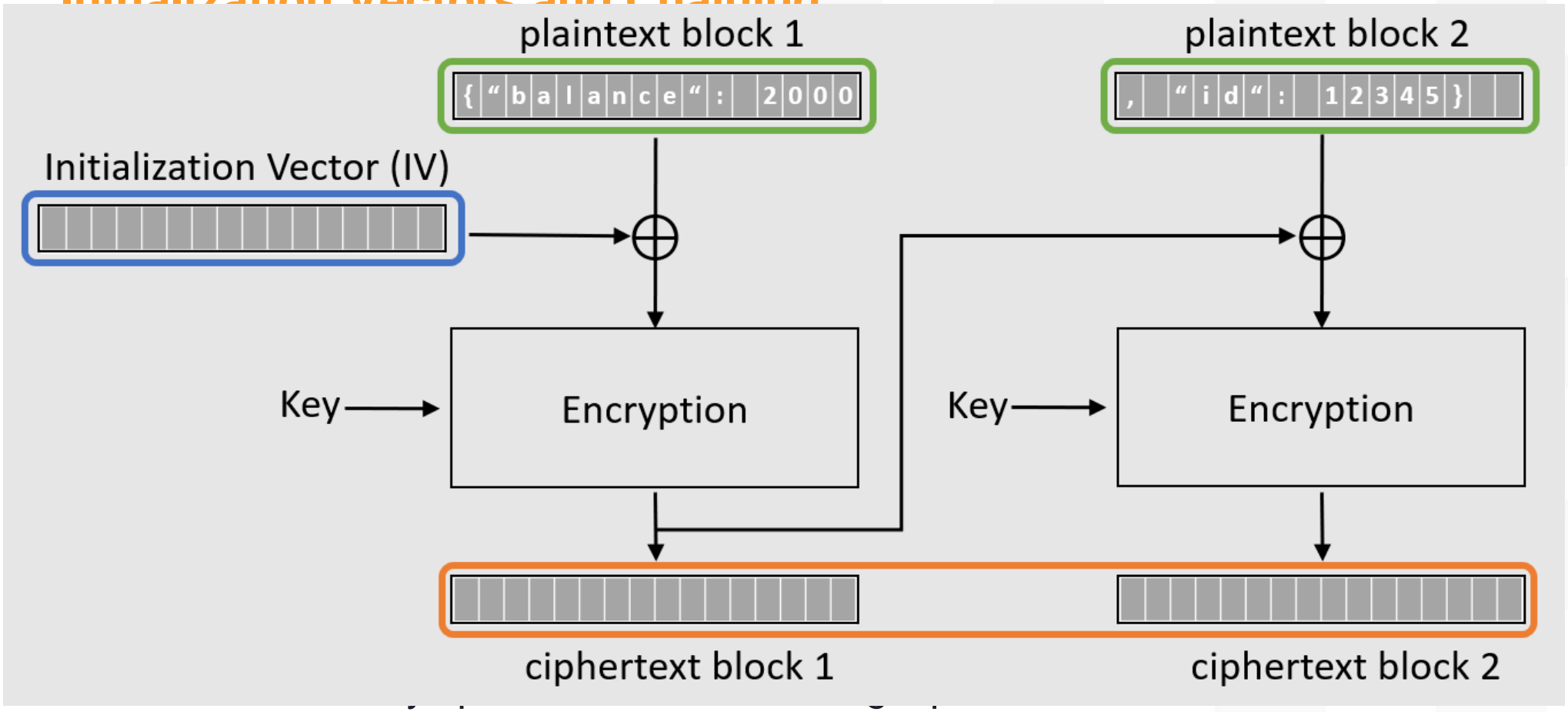
Initialization Vectors and Chaining

- Initialization vector (or "IV") is used in some symmetric ciphers to ensure that the first encrypted block of data is random.
  - Ensures that identical plaintexts encrypt to different ciphertexts
  - Two messages that begin the same will encrypt the same way up to the first difference. Some messages have a common header: a letterhead, or a 'From' line, or whatever."
- Chaining (*called* ***feedback*** *in stream modes*) seeds the previous encrypted block into the next block to be encrypted
  - Destroys patterns in the resulting ciphertext

LECTURE

Symmetric Encryption

Initialization Vectors and Chaining

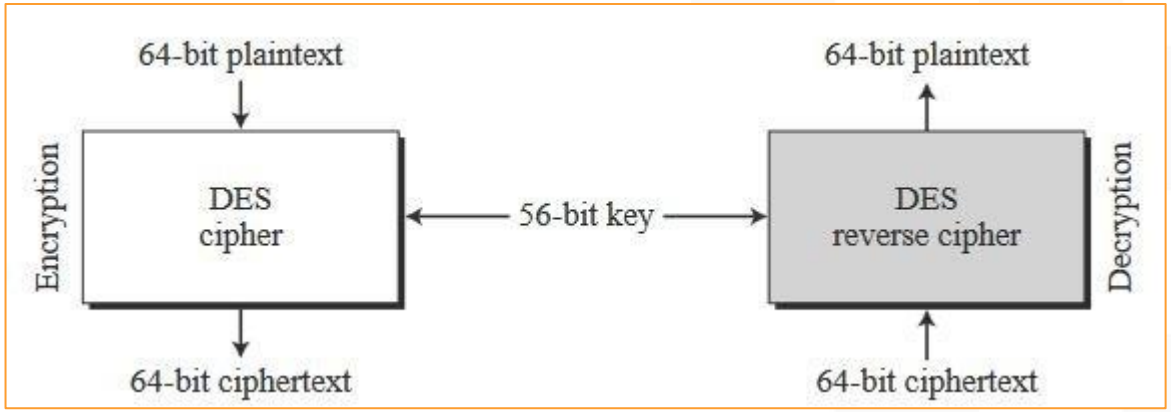


LECTURE

Symmetric Encryption

Data Encryption Standard (DES)

- DES is the Data Encryption Standard
- Describes the Data Encryption Algorithm (DEA)
- Made a United States federal standard symmetric cipher in 1976
- Designed by IBM, based on their older Lucifer symmetric cipher
- Uses a 64-bit block size (meaning it encrypts 64 bits each round) and a 56-bit key.



LECTURE

Symmetric Encryption

Data Encryption Standard (DES) - Modes

- DES can use **five different modes** to encrypt data
- The modes' primary difference is block versus (emulated) stream, the use of initialization vectors, and whether errors in encryption will propagate to subsequent blocks.
- The five modes of DES are:
  - **Electronic Code Book (ECB)**
  - **Cipher Block Chaining (CBC)**
  - **Cipher Feedback (CFB)**
  - **Output Feedback (OFB)**
  - **Counter Mode (CTR)**
- ECB is the original mode of DES
- CBC, CFB, and OFB were later added in FIPS Publication 81 (see http://www.itl.nist.gov/fipspubs/fip81.htm)
- CTR mode is the newest mode, described in NIST Special Publication 800-38a (see: http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf)

Notice the words "chaining" and "feedback"

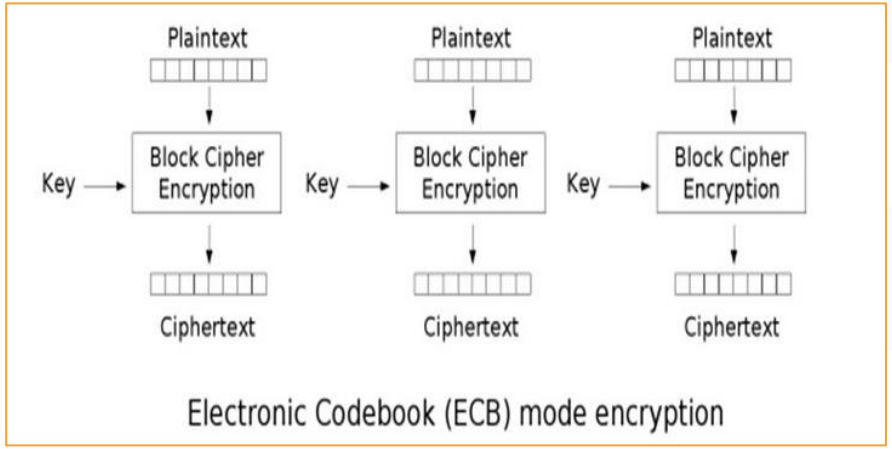
Block mode/Stream mode

LECTURE

Symmetric Encryption

Data Encryption Standard (DES) - Electronic Code Book (ECB)

- The simplest and **weakest** form of DES
- No initialization vector or chaining
- Identical plaintexts with identical keys encrypt to identical ciphertexts



Electronic Codebook (ECB) mode encryption

Lack of diffusion

Susceptible to replay attacks.

LECTURE

Symmetric Encryption

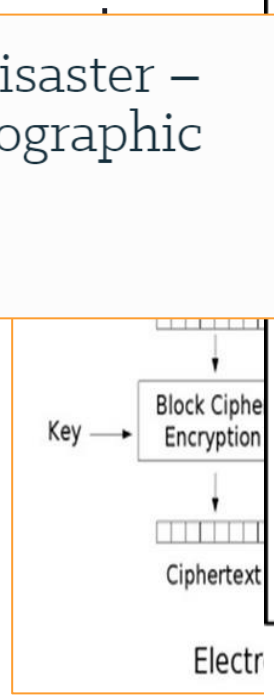
Data Encryption Standard (ECB)

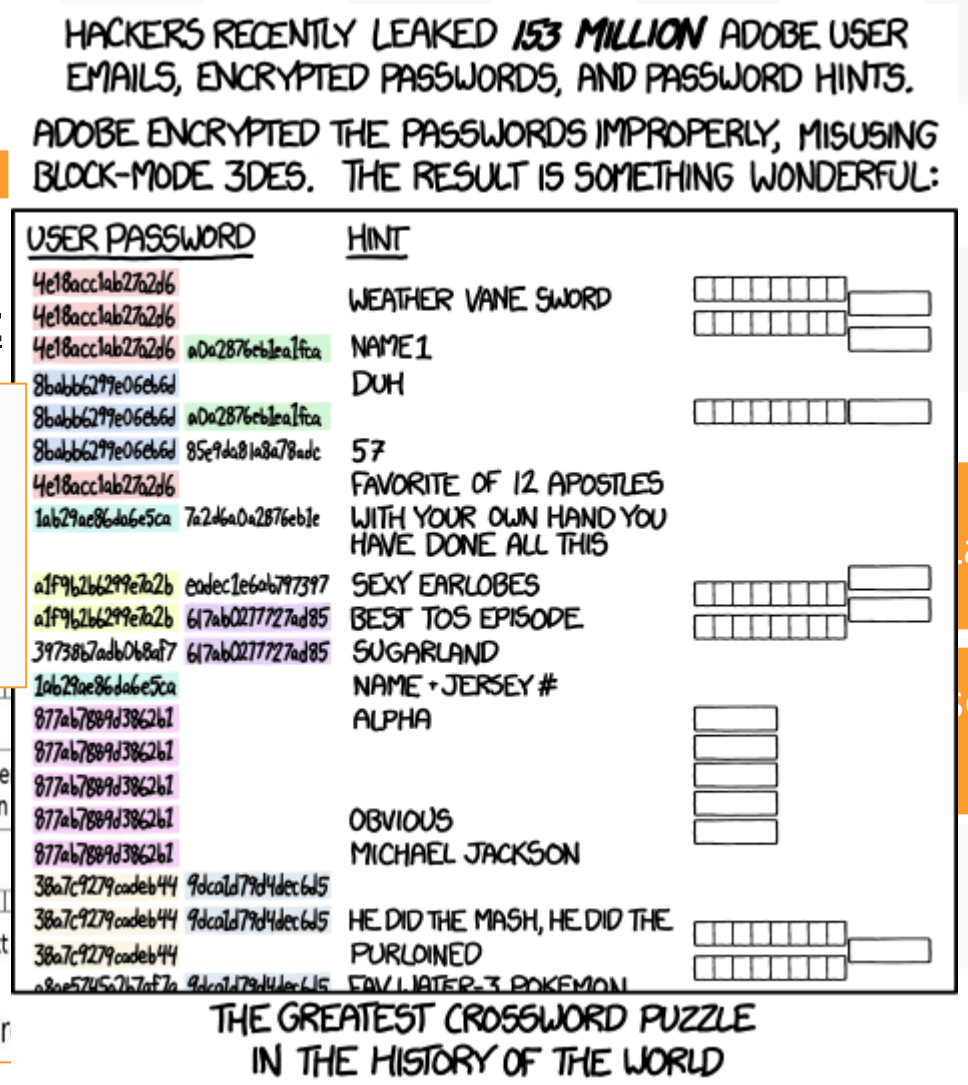
- The simplest and **weakest**

Anatomy of a password disaster – Adobe's giant-sized cryptographic blunder

04 NOV 2013 65

Adobe, Cryptography, Data loss, Privacy





ack of diffusion

ceptible to replay attacks.

LECTURE

Symmetric Encryption

Data Encryption Standard (DES) - Cipher Block Chaining (CBC)

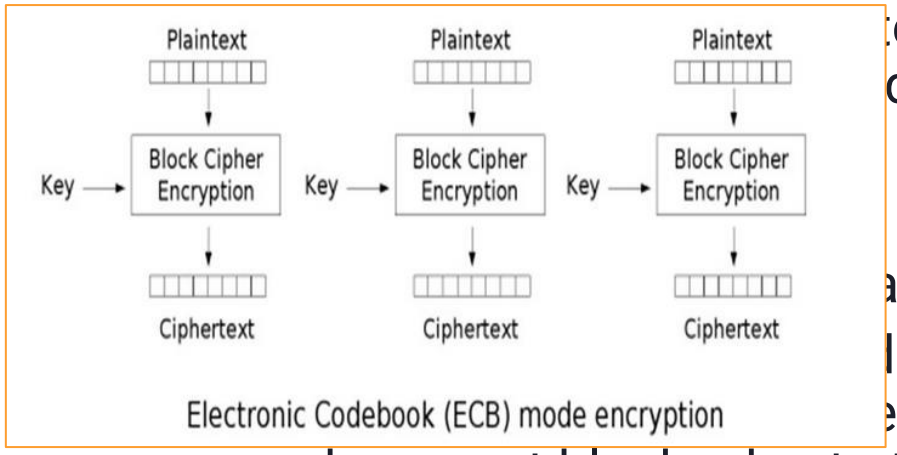
- A block mode of DES
- XORs the previous encrypted block of ciphertext to the next block of plaintext to be encrypted
- First encrypted block is an initialization vector that contains random data
- The “chaining” destroys patterns
- One limitation of CBC mode is that encryption **errors will propagate**: an encryption error in one block will cascade through subsequent blocks due to the chaining, destroying their integrity.

LECTURE

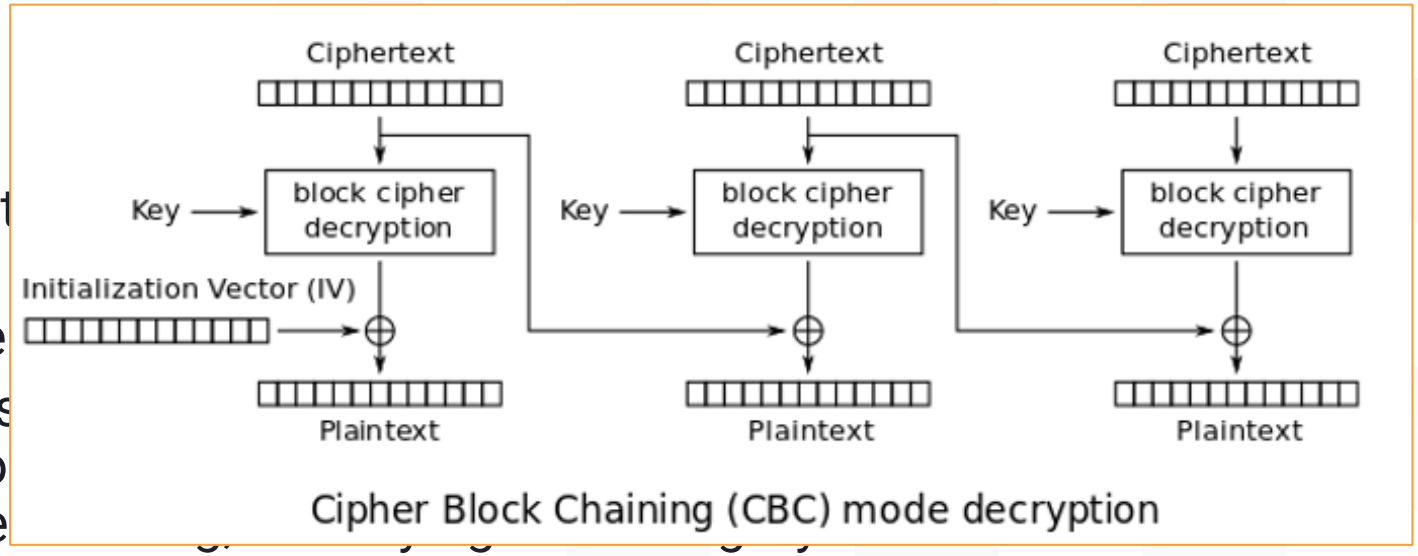
Symmetric Encryption

Data Encryption Standard (DES) - Cipher Block Chaining (CBC)

- A block mode of DES



Electronic Codebook (ECB) mode encryption



Cipher Block Chaining (CBC) mode decryption

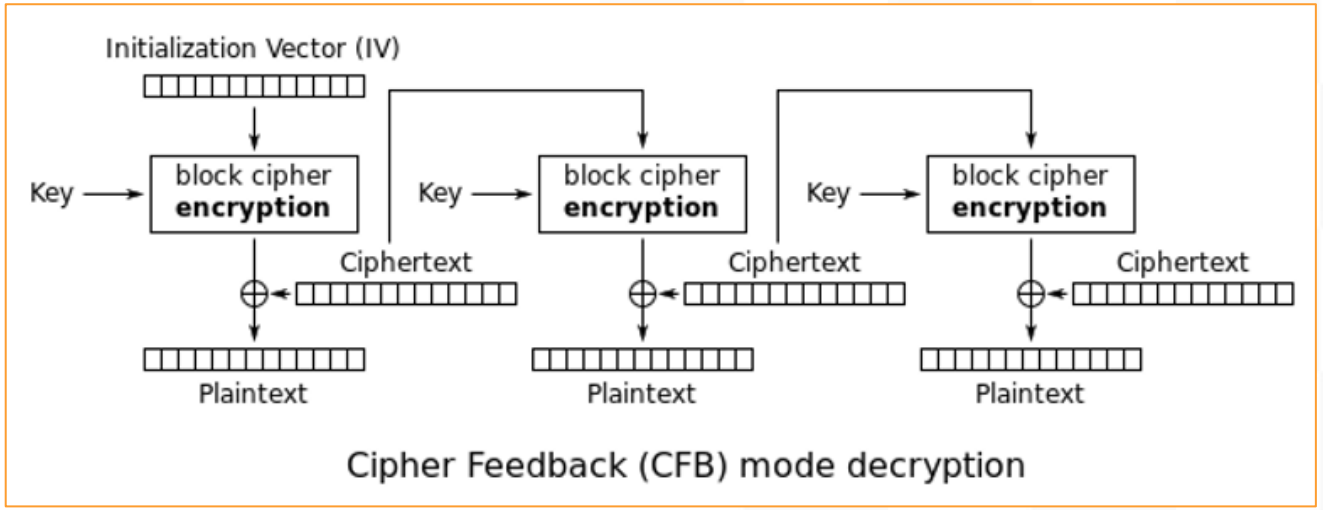
subsequent blocks due to the

LECTURE

Symmetric Encryption

Data Encryption Standard (DES) - Cipher Feedback (CFB)

- Very similar to CBC; the primary difference is CFB is a stream mode
- Uses feedback (the name for chaining when used in stream modes) to destroy patterns
- Like CBC, CFB uses an initialization vector and destroys patterns, and **errors propagate**



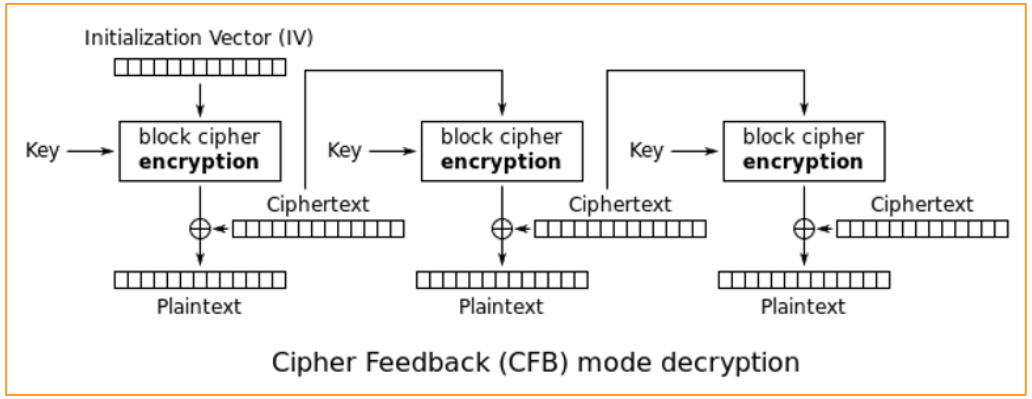
Cipher Feedback (CFB) mode decryption

LECTURE

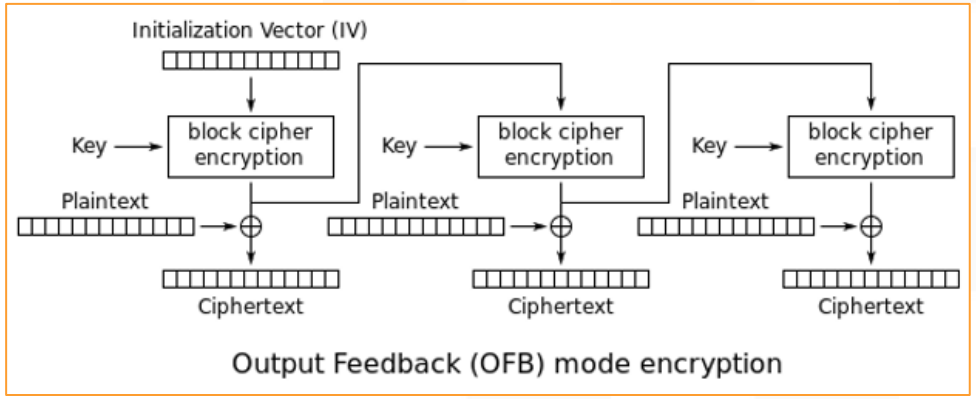
Symmetric Encryption

Data Encryption Standard (DES) - Output Feedback (OFB)

- Differs from CFB in the way feedback is accomplished
- CFB uses the previous ciphertext for feedback. The previous ciphertext is the subkey XORed to the plaintext.
- OFB uses the subkey before it is XORed to the plaintext.
- Since the subkey is not affected by encryption errors, **errors will not propagate**.



Cipher Feedback (CFB) mode decryption



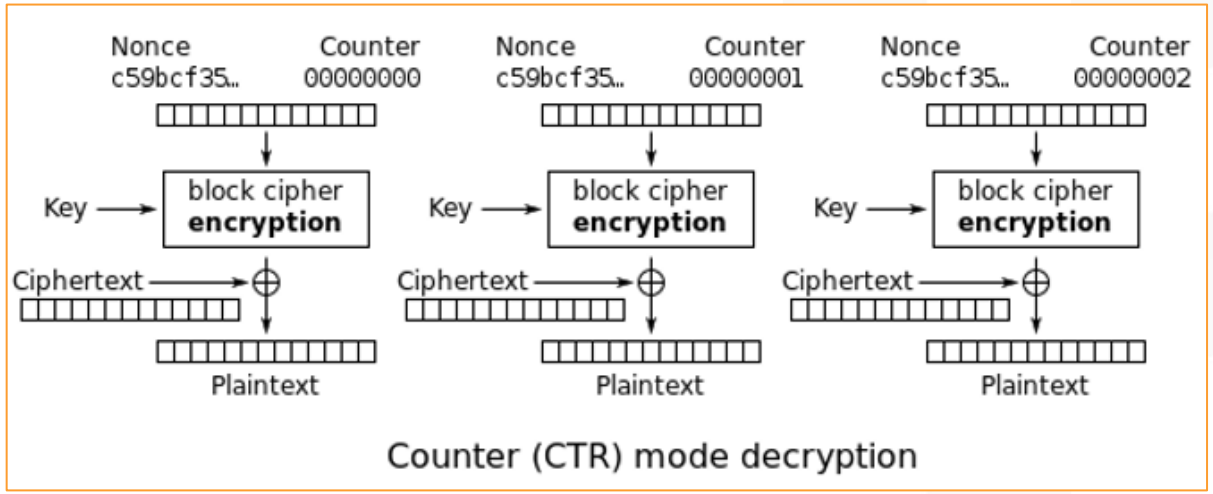
Output Feedback (OFB) mode encryption

LECTURE

Symmetric Encryption

Data Encryption Standard (DES) - Counter (CTR)

- Like OFB; the difference again is the feedback: CTRmode uses a counter
- Shares the same advantages as OFB (patterns are destroyed and errors do not propagate) with an additional advantage: since the feedback can be as simple as an ascending number, CTR mode encryption can be done in parallel



Counter (CTR) mode decryption

LECTURE

Symmetric Encryption

Data Encryption Standard (DES) – Modes Comparison Table

	Type	Initialization Vector	Error Propagation?
Electronic Code Book (ECB)	Block	No	No
Cipher Block Chaining (CBC)	Block	Yes	Yes
Cipher Feedback (CFB)	Stream	Yes	Yes
Output Feedback (OFB)	Stream	Yes	No
Counter Mode (CTR)	Stream	Yes	No

MEMORIZE, OK?

LECTURE

Symmetric Encryption

Data Encryption Standard (DES) – Single DES

- Original implementation of DES
- Encrypts 64-bit blocks of data with a 56-bit key, using 16 rounds of encryption
- Work factor required to break DES was reasonable in 1976
- Massively parallel computers such as COPACOBANA (*Cost-Optimized Parallel COde Breaker*, given as a nontestable example, see: http://www.copacobana.org for more information), which uses over 100 CPUs in parallel, can break 56-bit DES in a week or so (and faster with more CPUs), at a cost of under $10,000.

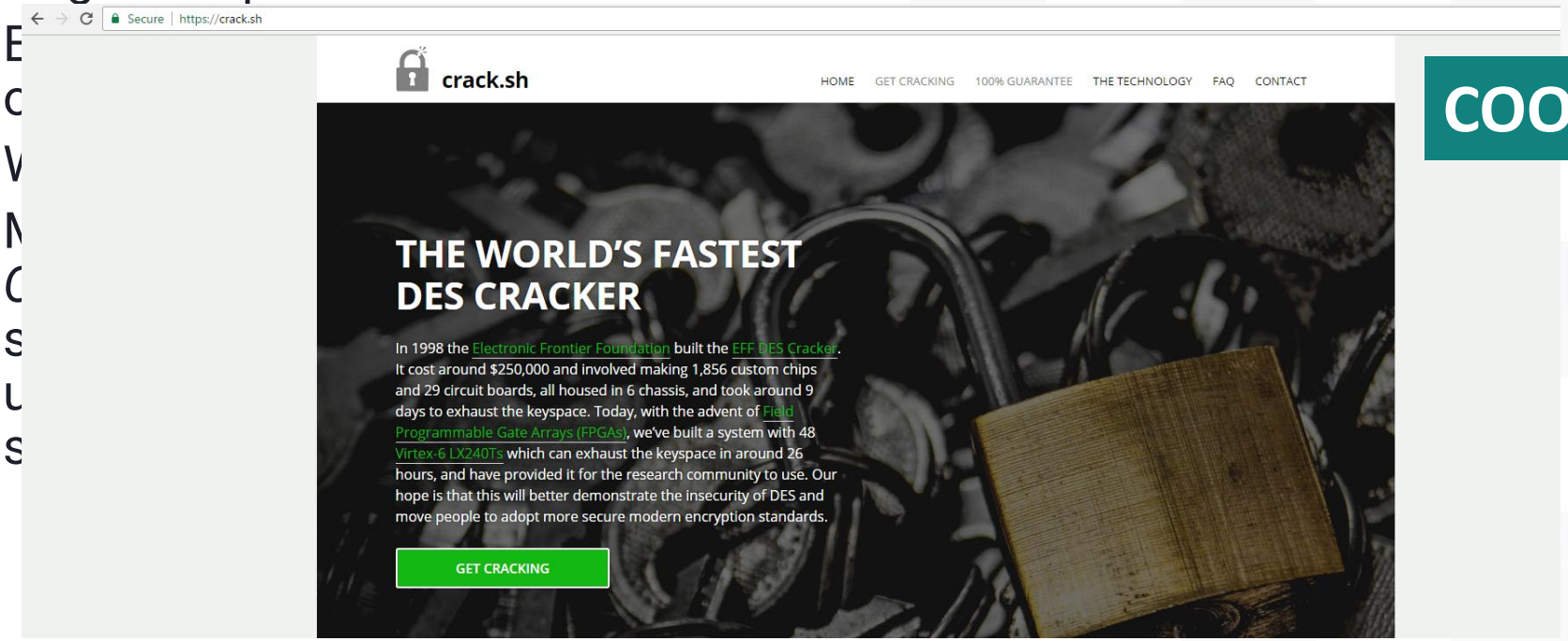
Today is less than 22 hours.

LECTURE

Symmetric Encryption

Data Encryption Standard (DES) – Single DES

- Original implementation of DES
- E
  C
- V
- M
  C
  S
  U
  S



COOL SITE!

LECTURE

Symmetric Encryption

Data Encryption Standard (DES) – Triple DES

- Applies single DES encryption three times per block
- Became a recommended standard in 1999 by the United States Federal Information Processing Standard (FIPS) Publication 46-3 (see: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf)
- The primary weakness is that it is slow and complex compared to newer symmetric algorithms such as AES or Twofish

NOTE: “Double DES” (applying DES encryption twice using two keys) is not used due to a meet-in-the-middle attack

LECTURE

Symmetric Encryption

FIPS Publication 46-3

ARCHIVED PUBLICATION

The attached publication,

FIPS Publication 46-3
(reaffirmed October 25, 1999),

was withdrawn on May 19, 2005 and is provided here only for historical purposes.

For related information, see:

- Special Publication 800-131A, *Transitions: Recommendations for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, http://csrc.nist.gov/publications/PubsSPs.html#800-131A;
- Special Publication 800-67 Rev. 1, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, http://csrc.nist.gov/publications/PubsSPs.html#800-67;
- FIPS Publication 197, *Advanced Encryption Standard*, http://csrc.nist.gov/publications/PubsFIPS.html#197; and
- NIST Cryptographic Toolkit: Block Ciphers, http://csrc.nist.gov/groups/ST/toolkit/block_ciphers.html.

LECTURE

Symmetric Encryption

Data Encryption Standard (DES) – Triple DES encryption order and keying options

- Applies DES encryption three times per block
- FIPS 46-3 describes "Encrypt, Decrypt, Encrypt" (EDE) order using three keying options: one, two, or three unique keys (called 1TDES EDE, 2TDES EDE, and 3TDES EDE, respectively)
- Applying triple DES EDE with the same key each time results in the same ciphertext as single DES
- 2TDES EDE uses key 1 to encrypt, key 2 to "decrypt," and key 1 to encrypt. This results in 112 bits of key length. It is commonly used for legacy hardware applications with limited memory
- 3TDES EDE (three different keys) is the strongest form, with 168 bits of key length
- Two- and three-key TDES EDE remain a FIPS-approved standard until 2030 (sort of)

LECTURE

Symmetric Encryption

Data Encryption Standard (DES) – Triple DES encryption order and keying options

Single DES encryption

Operation	Key	Input	Output
Encrypt	Hannibal	ATTACK AT DAWN	•ÁGPÚÂ ¦qŸÝ«¦

Triple DES Encryption with One Key

Operation	Key	Input	Output
Encrypt	Hannibal	ATTACK AT DAWN	•ÁGPÚÂ ¦qŸÝ«¦
Decrypt	Hannibal	•ÁGPÚÂ ¦qŸÝ«¦	ATTACK AT DAWN
Encrypt	Hannibal	ATTACK AT DAWN	•ÁGPÚÂ ¦qŸÝ«¦-

LECTURE

Symmetric Encryption

International Data Encryption Algorithm (IDEA)

- A symmetric block cipher designed as an international replacement to DES
- **Patented** in many countries
- Uses a 128-bit key and 64-bit block size
- Held up to cryptanalysis
- Primary drawbacks are patent encumbrance and its **slow** speed compared to newer symmetric ciphers such as AES

LECTURE

Symmetric Encryption

Advanced Encryption Standard (AES)

- Current United States standard symmetric block cipher
- Federal Information Processing Standard (FIPS) 197 (see: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf)
- Uses 128-bit (with 10 rounds of encryption), 192-bit (12 rounds of encryption), or 256-bit (14 rounds of encryption) keys to encrypt 128-bit blocks of data
- Open algorithm, free to use, and free of any intellectual property restrictions
- Designed to replace DES

LECTURE

Symmetric Encryption

Advanced Encryption Standard (AES) - Choosing AES

- National Institute of Standards and Technology (NIST) solicited input on a replacement for DES in the Federal Register in January 1997
- Fifteen AES candidates were announced in August 1998
- List was reduced to five in August 1999
- Rijndael was chosen and became AES

Pioneering names in encryption

Five AES Finalists

Name	Author
MARS	IBM (11 authors)
RC6	RSA (Rivest, Robshaw, Sidney, Yin)
Rijndael	Daemen, Rijmen
Serpent	Anderson, Biham, Knudsen
Twofish	Schneier, Kelsey, Hall, Ferguson, Whiting, Wagner

LECTURE

Symmetric Encryption

Advanced Encryption Standard (AES) - AES functions

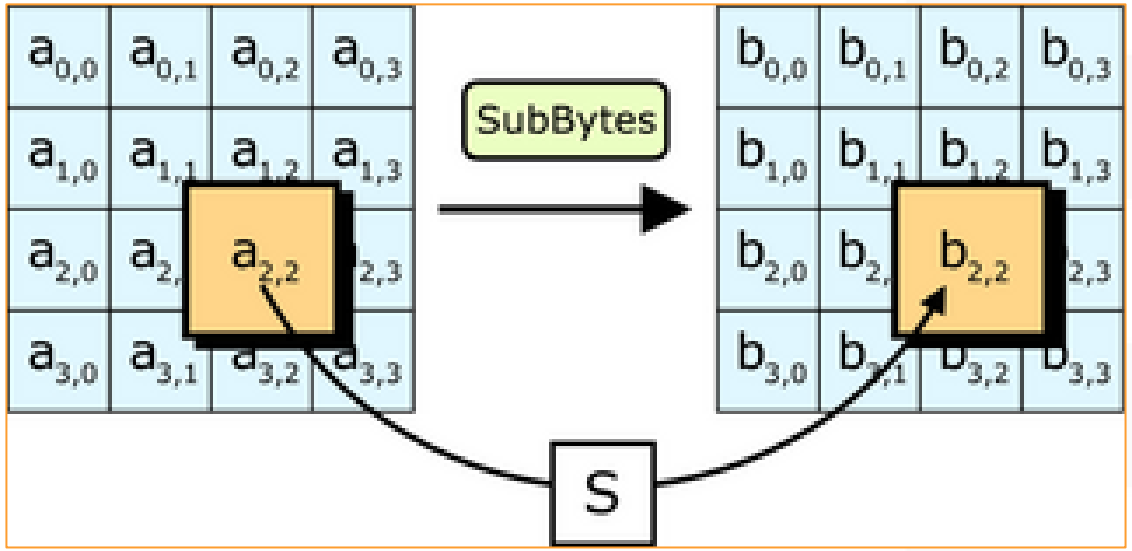
- AES has four functions:
  - SubBytes
  - ShiftRows
  - MixColumns
  - AddRoundKey
- Operates on data called a “State” – 4 rows of 4 16 byte blocks

LECTURE

Symmetric Encryption

Advanced Encryption Standard (AES) - AES functions - SubBytes

- Provides confusion by substituting the bytes of the State
- Bytes are substituted according to a substitution table (also called an S-Box)

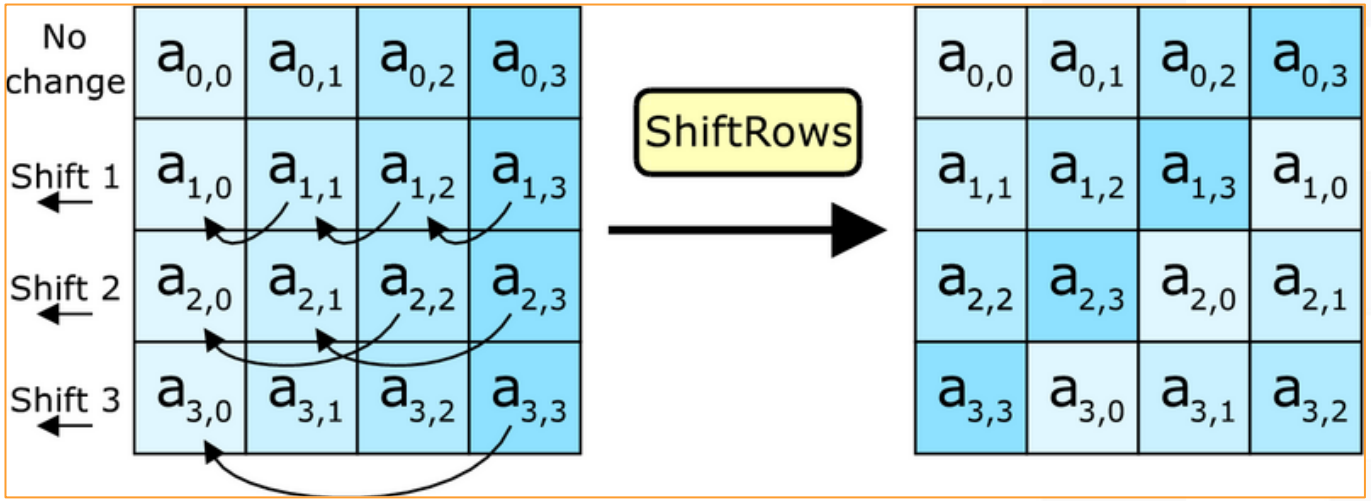


LECTURE

Symmetric Encryption

Advanced Encryption Standard (AES) - AES functions - ShiftRows

- Provides **diffusion** by shifting rows of the State (block of data that is being encrypted via AES)

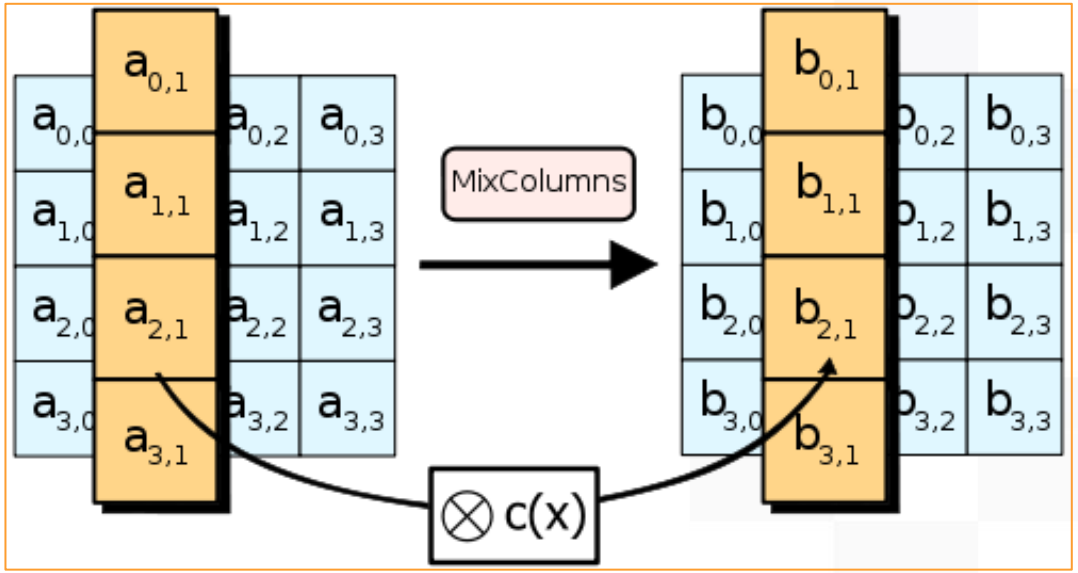


LECTURE

Symmetric Encryption

Advanced Encryption Standard (AES) - AES functions - MixColumns

- Provides **diffusion** by “mixing” the columns of the State via finite field mathematics

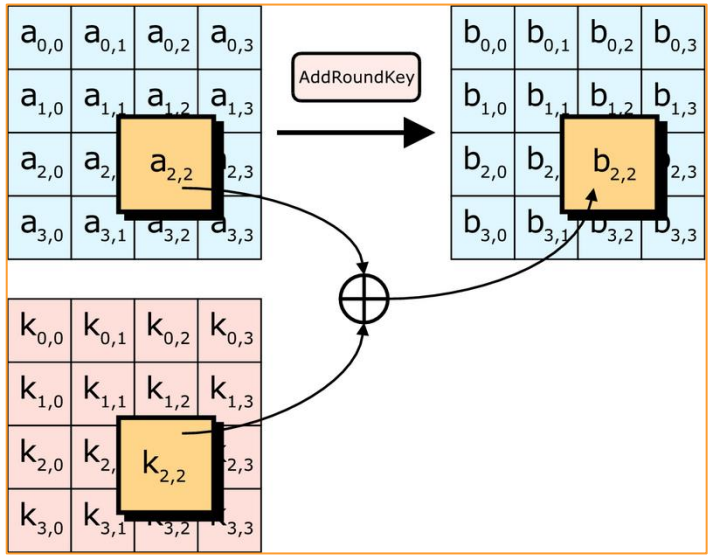


LECTURE

Symmetric Encryption

Advanced Encryption Standard (AES) - AES functions - AddRoundKey

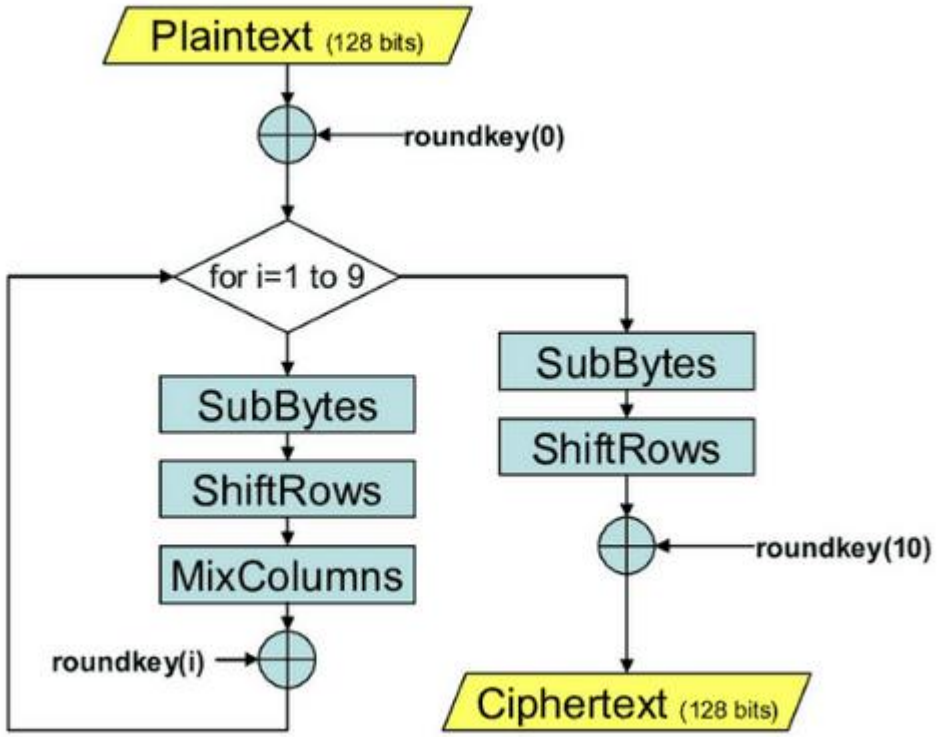
- **Final function applied in each round**
- **XOR**s the State with the subkey
- Subkey is derived from the key, and is different for each round of AES



LECTURE

Symmetric Encryption

Advanced Encryption Standard (AES) - AES functions – All Together



- 10 rounds are required for a 128-bit key
- 12 Rounds are required for a 192-bit key
- 14 Rounds are required for a 256-bit key

LECTURE

Symmetric Encryption

Blowfish and Twofish

- Symmetric **block cipher**s created by teams lead by Bruce Schneier
- Blowfish uses from 32 through 448 bit (the default is 128) keys to encrypt 64 bits of data
- Twofish was an AES finalist, encrypting 128-bit blocks using 128 through 256 bit keys
- Both are open algorithms, unpatented and freely available

CISSP® MENTOR PROGRAM – SESSION FIVE

LECTURE

Symmetric Encryption

Blowfish and Twofish

- Symmetric block ciphers created by teams lead by Bruce

CISSP® MENTOR PROGRAM – SESSION FIVE

LECTURE

Symmetric Encryption

Blowfish and Twofish

LECTURE

Symmetric Encryption

RC5 and RC6

- Symmetric **block cipher**s by RSA Laboratories
- RC5 uses 32 (testing purposes), 64 (replacement for DES), or 128-bit blocks. The key size ranges from zero to 2040 bits.
- RC6 was an AES finalist. It is based on RC5, altered to meet the AES requirements. It is also stronger than RC5, encrypting 128-bit blocks using 128-, 192-, or 256-bit keys.

LECTURE

Symmetric Encryption

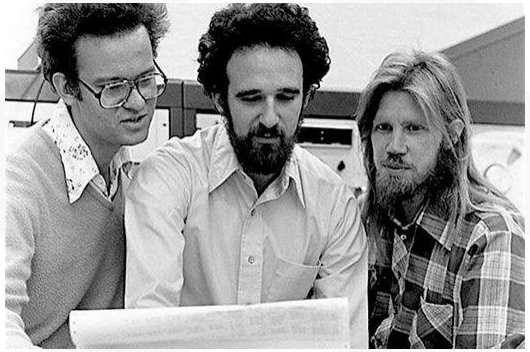
Think you got symmetric encryption down?

Now, asymmetric…

Algorithm	Type	Method	Key Size
AES	Symmetric encryption	128-bit block cipher	128-, 192-, or 256-bit key
DES	Symmetric encryption	64-bit block cipher	56-bit key
3DES	Symmetric encryption	64-bit block cipher	56-, 112-, or 168-bit key
Blowfish	Symmetric encryption	64-bit block cipher	32- to 448-bit key
Twofish	Symmetric encryption	128-bit block cipher	128-, 192-, or 256-bit key
RC4	Symmetric encryption	Stream cipher	40- to 2,048-bit key

LECTURE

Asymmetric Encryption

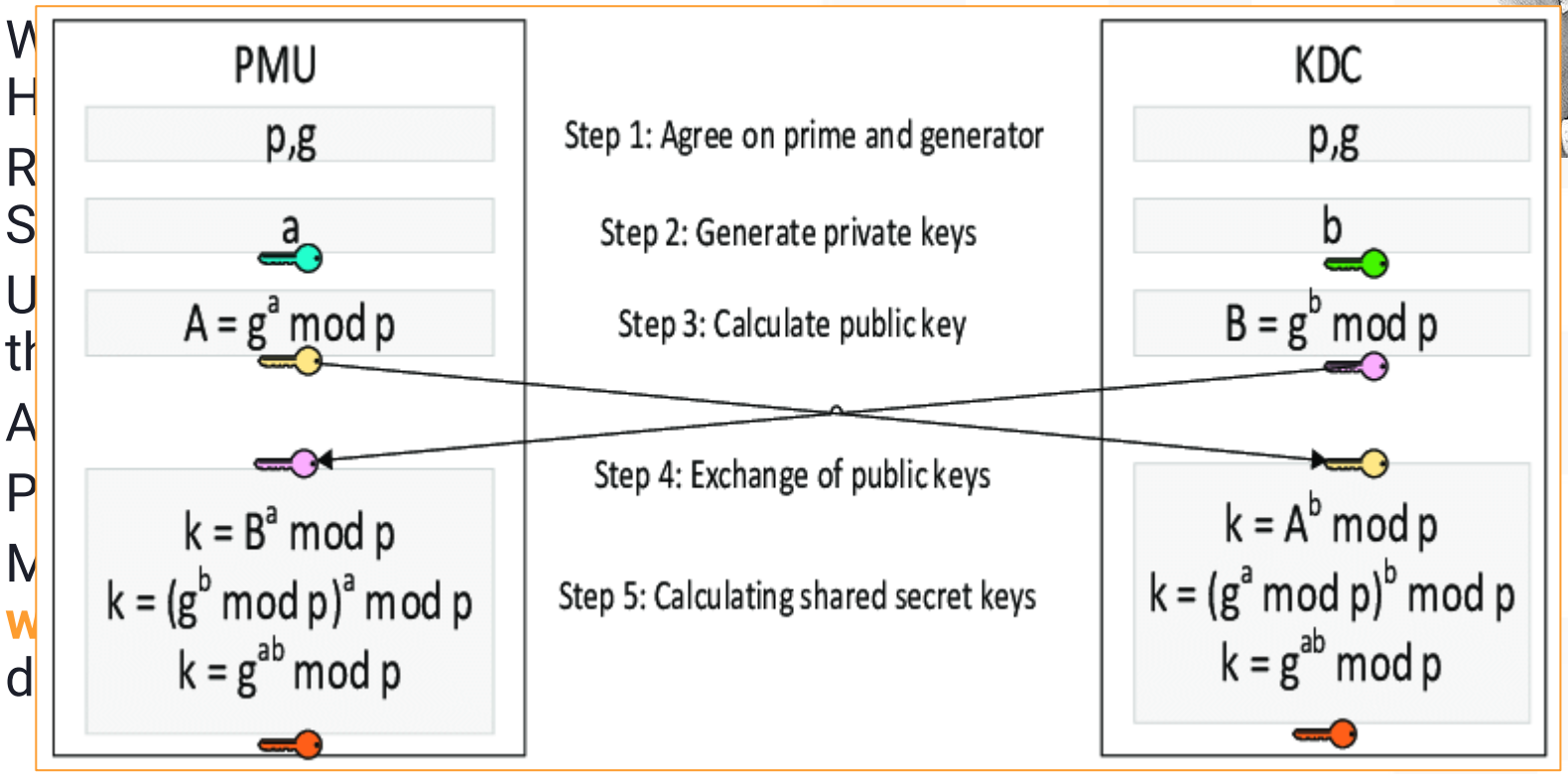


- Solves the age-old challenge of preshared keys
- Whitfield Diffie and Martin Hellman, who created the Diffie-Hellman key exchange in 1976
- RSA algorithm was invented in 1977 (RSA stands for “Rivest, Shamir, and Adleman,” the authors’ names)
- Uses **two keys**: if you encrypt with one key, you may decrypt with the other
- Also called public key encryption
- Public – Private key pair
- Math lies behind the asymmetric encryption - methods use “**one-way functions**,” which are easy to compute “one way,” and difficult to compute in the reverse direction.

LECTURE

Asymmetric Encryption

- Solves the age-old challenge of preshared keys
- W
  H
- R
  S
- U
  th
- A
- P
- M
  w
  d



LECTURE

Asymmetric Encryption

Methods (there are two primary ones)

Math lies behind the asymmetric encryption - methods use “one-way functions,” which are easy to compute “one way,” and difficult to compute in the reverse direction.

Factoring Prime Numbers

- Factoring a composite number into its primes
- Prime number is a number evenly divisible only by one and itself
- Composite number is evenly divisible by numbers other than 1 and itself.
- Multiplying the prime number 6269 by the prime number 7883 results in the composite number 49,418,527. That “way” is quite easy to compute, taking milliseconds on a calculator. Answering the question “which prime number times which prime number equals 49,418,527” is much more difficult.
- The problem is called factoring, and no shortcut has been found for hundreds of years
- Basis of the RSA algorithm
- Factoring a large composite number (one thousands of bits long) is so difficult that the composite number can be safely publicly posted (this is the public key).
- The primes that are multiplied to create the public key must be kept private (they are the private key).

LECTURE

Asymmetric Encryption

Methods (there are two primary ones)

Math lies behind the asymmetric encryption - methods use “one-way functions,” which are easy to compute “one way,” and difficult to compute in the reverse direction.

Discrete Logarithm

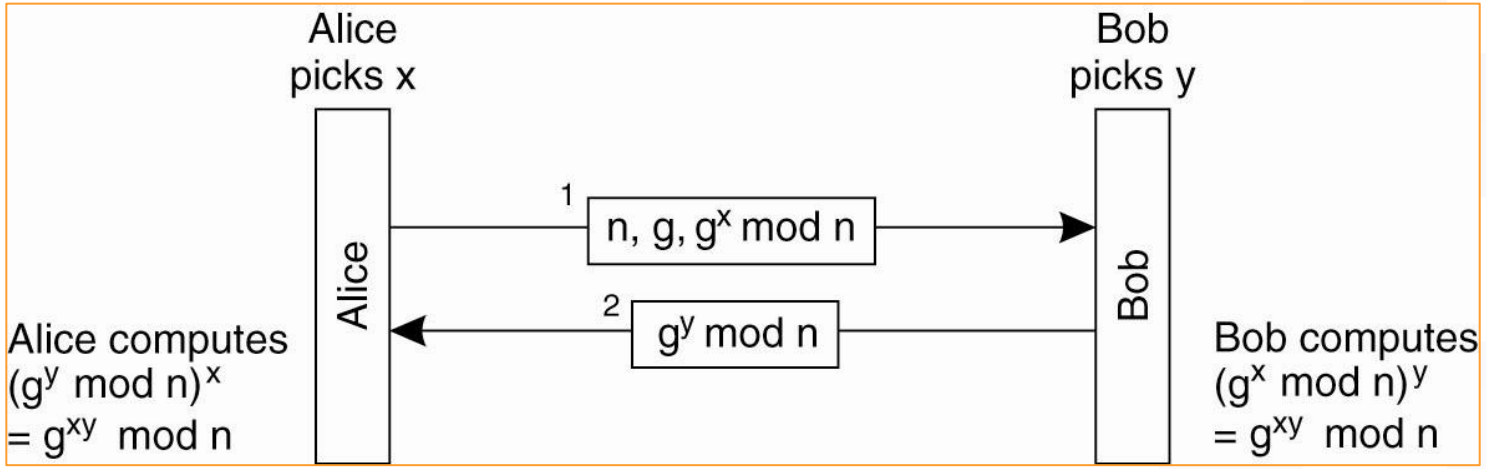
- A logarithm is the opposite of exponentiation
- Computing 7 to the 13th power (exponentiation) is easy on a modern calculator: 96,889,010,407. Asking the question “96,889,010,407 is 7 to what power” (finding the logarithm) is more difficult
- Basis of the Diffie-Helmann and ElGamal asymmetric algorithms

LECTURE

Asymmetric Encryption

Diffie-Hellman key agreement protocol

- Allows two parties to securely agree on a symmetric key via a public channel
- Also called the Diffie-Hellman Key Exchange



LECTURE

Asymmetric Encryption

Elliptic Curve Cryptography (ECC)

- One-way function that uses **discrete logarithms as applied to elliptic curves**
- Solving this problem is harder than solving discrete logarithms, so algorithms based on Elliptic Curve Cryptography (ECC) are **much stronger** per bit than systems using discrete logarithms (and also stronger than factoring prime numbers)
- Requires **less computational resources** because shorter keys can be used compared to other asymmetric methods
- Often **used in lower power devices**

LECTURE

Asymmetric Encryption

Asymmetric and Symmetric Tradeoffs

- Asymmetric encryption is far slower than symmetric encryption
- Asymmetric encryption is weaker per bit of key length
- Asymmetric and symmetric encryption are typically used together: use an asymmetric algorithm such as RSA to securely send someone an AES (symmetric) key

Symmetric Versus Asymmetric Strength[8]

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	15,360	15,360	512+

LECTURE

Hash Functions

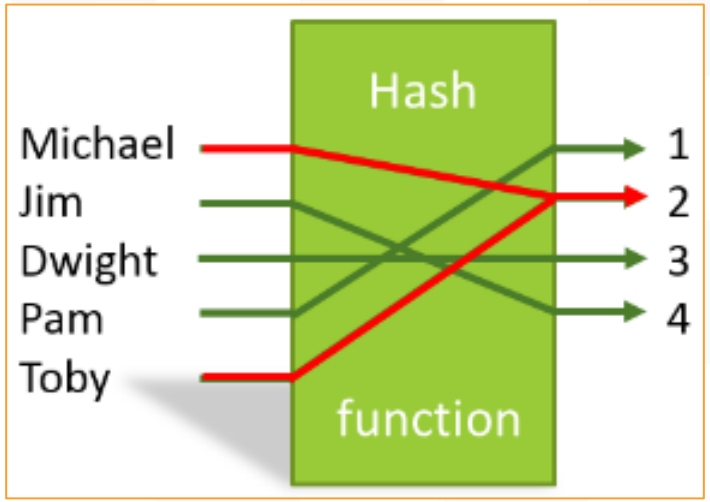
- Provides encryption using an algorithm and **no key**
- Called "**one-way** hash functions" because there is no way to reverse the encryption
- A **variable-length plaintext is "hashed" into a fixed-length hash value** (often called a "message digest" or a "hash")
- Primarily used to provide integrity: if the hash of a plaintext changes, the plaintext itself has changed
- Older hash functions include Secure Hash Algorithm 1 (SHA-1), which creates a 160-bit hash and Message Digest 5 (MD5), which creates a 128-bit hash
- Newer alternatives such as SHA-2 are recommended

LECTURE

Hash Functions

Collisions

- Hashes are not unique, because the number of possible plaintexts is far larger than the number of possible hashes
- More than one document could have the same hash: this is called a collision
- Collisions are always possible (assuming the plaintext is longer than the hash), they should be very difficult to find



LECTURE

Hash Functions

MD5

- Message Digest algorithm 5, created by Ronald Rivest
- Creates a 128-bit hash value based on any input length
- Weaknesses have been discovered where collisions could be found in a practical amount of time
- MD6 is the newest version of the MD family of hash algorithms, first published in 2008

LECTURE

Hash Functions

Secure Hash Algorithm (SHA)

- Name of a series of hash algorithms
- SHA-1 was announced in 1993 in the United States Federal Information Processing Standard 180 (see http://www.itl.nist.gov/fipspubs/fip180-1.htm)
- SHA-1 creates a 160-bit hash value
- SHA-2 is recommended over SHA-1 or MD5
- The SHA-3 competition was announced in the Federal Register in 2007; SHA-3 was announced as a standard in the Fall of 2015 - Keccak algorithm (http://csrc.nist.gov/publications/drafts/fips-202/fips_202_draft.pdf)

LECTURE

Hash Functions

HAVAL

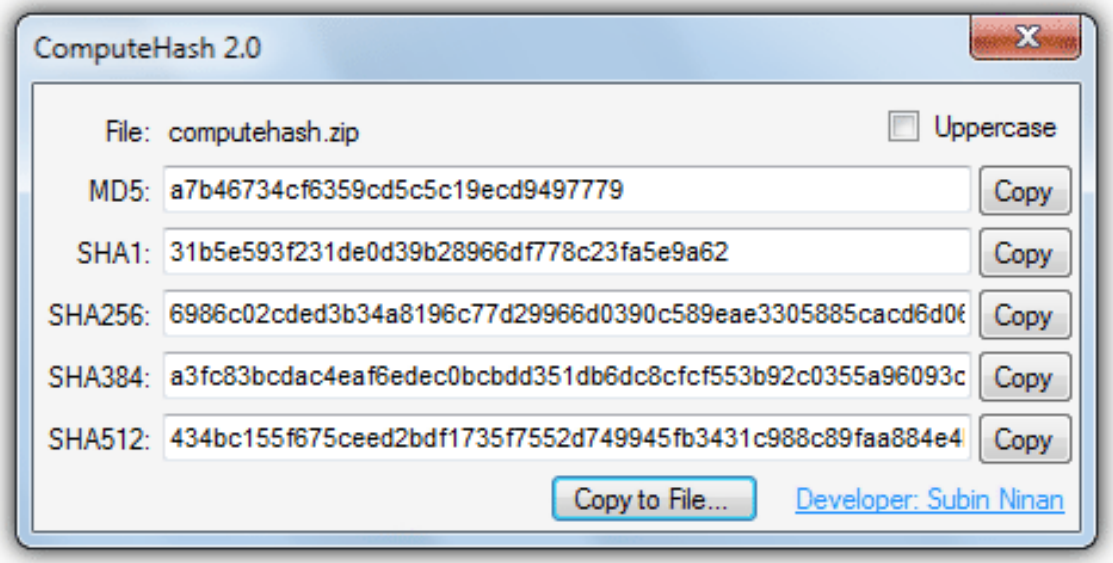
- Hash of Variable Length
- Creates message digests of 128, 160, 192, 224, or 256 bits in length, using 3, 4, or 5 rounds
- Uses some of the design principles behind the MD family of hash algorithms, and is faster than MD5

LECTURE

Hash Functions

HAVAL

- Hash of Variable Length
- Create bits in length
- Uses s ily of hash algorit



LECTURE

Cryptographic Attacks

Used by **cryptanalysts** to recover the plaintext without the key or to recover the key itself

Brute Force

- Generates the entire keyspace, which is every possible key
- Given enough time, the plaintext will be recovered
- Effective attack against all key-based ciphers, except for the one-time pad

LECTURE

Cryptographic Attacks

Used by **cryptanalysts** to recover the plaintext without the key or to recover the key itself

Known Plaintext

- Relies on recovering and analyzing a matching plaintext and ciphertext pair
- The goal is to derive the key which was used

Chosen Plaintext and Adaptive Chosen Plaintext

- Cryptanalyst chooses the plaintext to be encrypted
- Goal is to derive the key
- Adaptive-chosen plaintext begins with a chosen plaintext attack in round 1. The cryptanalyst then “adapts” further rounds of encryption based on the previous round

LECTURE

Cryptographic Attacks

Used by **cryptanalysts** to recover the plaintext without the key or to recover the key itself

Chosen Ciphertext and Adaptive Chosen Ciphertext

- Mirror chosen plaintext attacks: the difference is that the cryptanalyst chooses the ciphertext to be decrypted
- Usually launched against asymmetric cryptosystems

Meet-in-the-middle Attack

- Meet-in-the-middle attack encrypts on one side, decrypts on the other side, and meets in the middle
- Common attack is against “double DES”
- Attack is a known plaintext attack: the attacker has a copy of a matching plaintext and ciphertext, and seeks to recover the two keys used to encrypt.

LECTURE

Cryptographic Attacks

Used by **cryptanalysts** to recover the plaintext without the key or to recover the key itself

Known Key

- Known key means the cryptanalyst knows something about the key, to reduce the efforts used to attack it.
- If the cryptanalyst knows that the key is an uppercase letter and a number only, other characters may be omitted in the attack.

Differential Cryptanalysis

- Seeks to find the “difference” between related plaintexts that are encrypted
- Usually launched as an adaptive chosen plaintext attack
- The cryptanalyst uses statistical analysis to search for signs of nonrandomness in the ciphertexts

LECTURE

Cryptographic Attacks

Used by **cryptanalysts** to recover the plaintext without the key or to recover the key itself

Linear Cryptanalysis

- A known plaintext attack where the cryptanalyst finds large amounts of plaintext/ciphertext pairs created with the same key
- The pairs are studied to derive information about the key used to create them

Side-channel Attacks

Use physical data to break a cryptosystem, such as monitoring CPU cycles or power consumption used while encrypting or decrypting

LECTURE

Cryptographic Attacks

Used by **cryptanalysts** to recover the plaintext without the key or to recover the key itself

Birthday Attack

- Named after the birthday paradox
- Based on fact that in a room with 23 people or more, the odds are greater than 50% that two will share the same birthday
- The birthday paradox illustrates why many people's instinct on probability (and risk) is wrong. You are not trying to match a specific birthday (such as yours); you are trying to match any birthday.
- Used to create hash collisions

Key Clustering

Occurs when two different symmetric keys applied to the same plaintext produce the same ciphertext

LECTURE

Implementing Cryptography

Digital Signatures

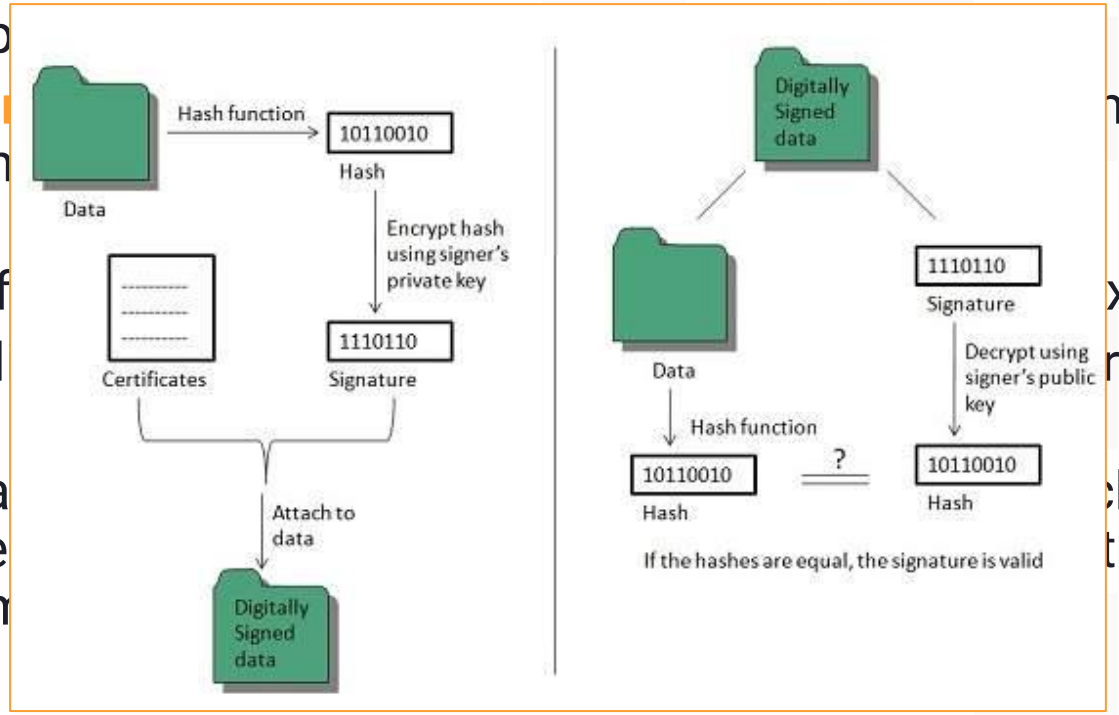
- Used to cryptographically sign documents
- Provide **nonrepudiation**, which includes authentication of the identity of the signer, and proof of the document's integrity (proving the document did not change)
- Use a hash function to generate a hash value of the plaintext
- Create the digital signature by encrypting the hash with a private key
- Digital signatures provide authentication and integrity, which forms nonrepudiation. They do not provide confidentiality: the plaintext remains unencrypted.

LECTURE

Implementing Cryptography

Digital Signatures

- Used to cryp
- Provide **nonr** identity of th (proving the
- Use a hash f
- Create the d key
- Digital signa forms nonre plaintext ren



LECTURE

Implementing Cryptography

HMAC

- Combines symmetric encryption with hashing
- Similar to a digital signature, except that it uses symmetric encryption instead of asymmetric
- HMACs are used by IPsec
- Two parties must preshare a secret key (such as a DES key). Once shared, the sender may generate a HMAC by hashing the message with an algorithm such as MD5 or SHA-1, and then encrypting the hash with the preshared key via symmetric cipher such as DES
- The receiver hashes the plaintext locally and also decrypts the HMAC with his/her copy of the private key, recovering the sender's hash. If the two hashes match, the sender is authenticated, and the message's integrity is assured.

LECTURE

Implementing Cryptography

Public Key Infrastructure (PKI)

- Leverages all three forms of encryption to provide and manage digital certificates
- A digital certificate is a public key signed with a digital signature
- Digital certificates may be server-based (used for SSL Web sites such as https://www.ebay.com, for example) or client-based (bound to a person).
- If the two are used together, they provide mutual authentication and encryption.
- The standard digital certificate format is X.509.

LECTURE

Implementing Cryptography

Public Key Infrastructure (PKI)

Certificate Authorities

- Digital certificates are issued by Certificate Authorities (CAs)
- Authenticate the identity of a person or organization before issuing a certificate to them
- CAs may be private (run internally) or public (such as Verisign or Thawte)

Certificate Revocation Lists

- Certificate Authorities maintain Certificate Revocation Lists (CRL)
- List certificates that have been revoked

LECTURE

Implementing Cryptography

IPSec

- **Suite of protocols** that provide a cryptographic layer to both IPv4 and IPv6
- One of the methods used to provide Virtual Private Networks (VPN)
- Includes two primary protocols:
  - **Authentication Header (AH)** and
  - **Encapsulating Security Payload (ESP)**.
- AH and ESP provide different, and sometimes overlapping functionality
- Supporting IPsec protocols include Internet Security Association and Key Management Protocol (ISAKMP) and Internet Key Exchange (IKE)

LECTURE

Implementing Cryptography

IPSec

AH and ESP

- Authentication Header provides authentication and integrity for each packet of network data
- AH provides no confidentiality; it acts as a digital signature for the data
- AH also protects against replay attacks
- Encapsulating Security Payload primarily provides confidentiality by encrypting packet data

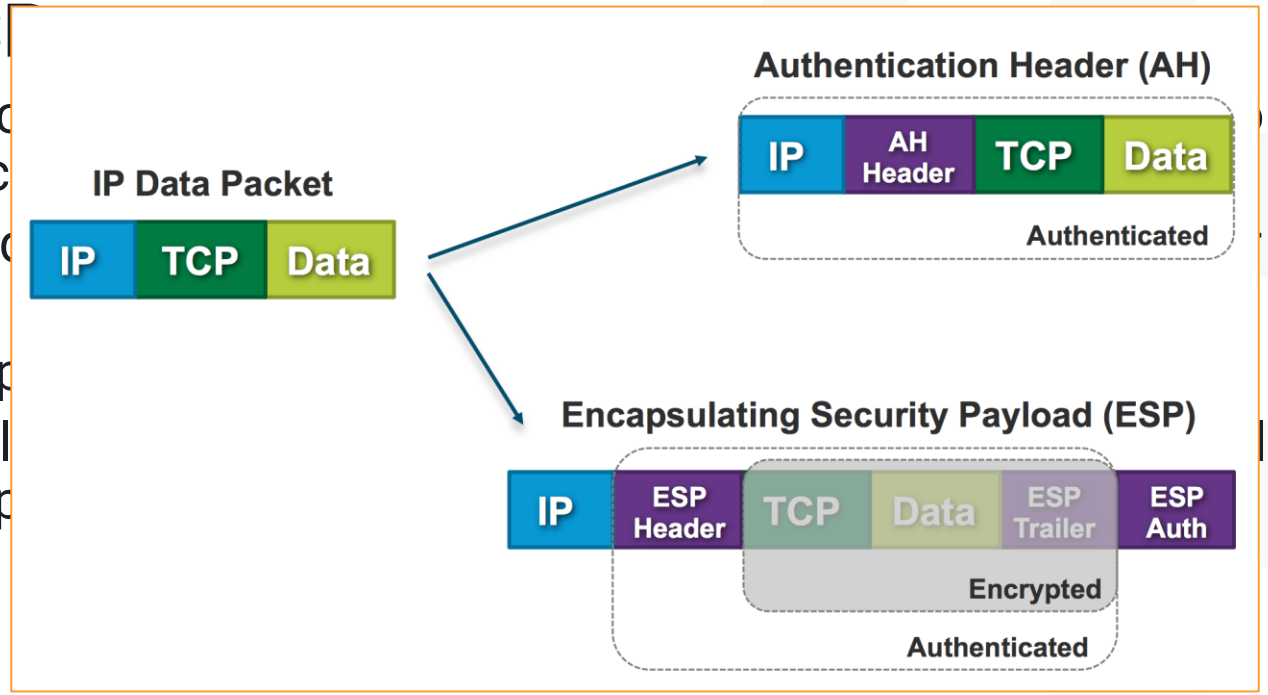
LECTURE

Implementing Cryptography

IPSec

AH and ES

- Authentic
  each pac
- AH provi
  the data
- AH also p
- Encapsul
  by encryp



LECTURE

Implementing Cryptography

IPSec

Security Association and ISAKMP

- An IPsec Security Association (SA) is a simplex (one-way) connection which may be used to negotiate ESP or AH parameters
- If two systems communicate via ESP, they use two SAs (one for each direction). If the systems leverage AH in addition to ESP, they use two more SAs, for a total of four
- Each simplex SA connection is identified by a unique 32-bit number called the Security Parameter Index (SPI)
- The SA process is managed by the Internet Security Association and Key Management Protocol (ISAKMP)

LECTURE

Implementing Cryptography

IPSec

Tunnel and Transport Mode

- IPsec can be used in tunnel mode or transport mode
- Tunnel mode is used by security gateways (which can provide point-to-point IPsec tunnels)
- ESP Tunnel mode encrypts the entire packet, including the original packet headers
- ESP Transport mode only encrypts the data (and not the original headers); this is commonly used when the sending and receiving system can “speak” IPsec natively

LECTURE

Implementing Cryptography

IPSec

Tunnel a

- IPsec
- Tunne
- ESP T
- ESP T

vide

point-t

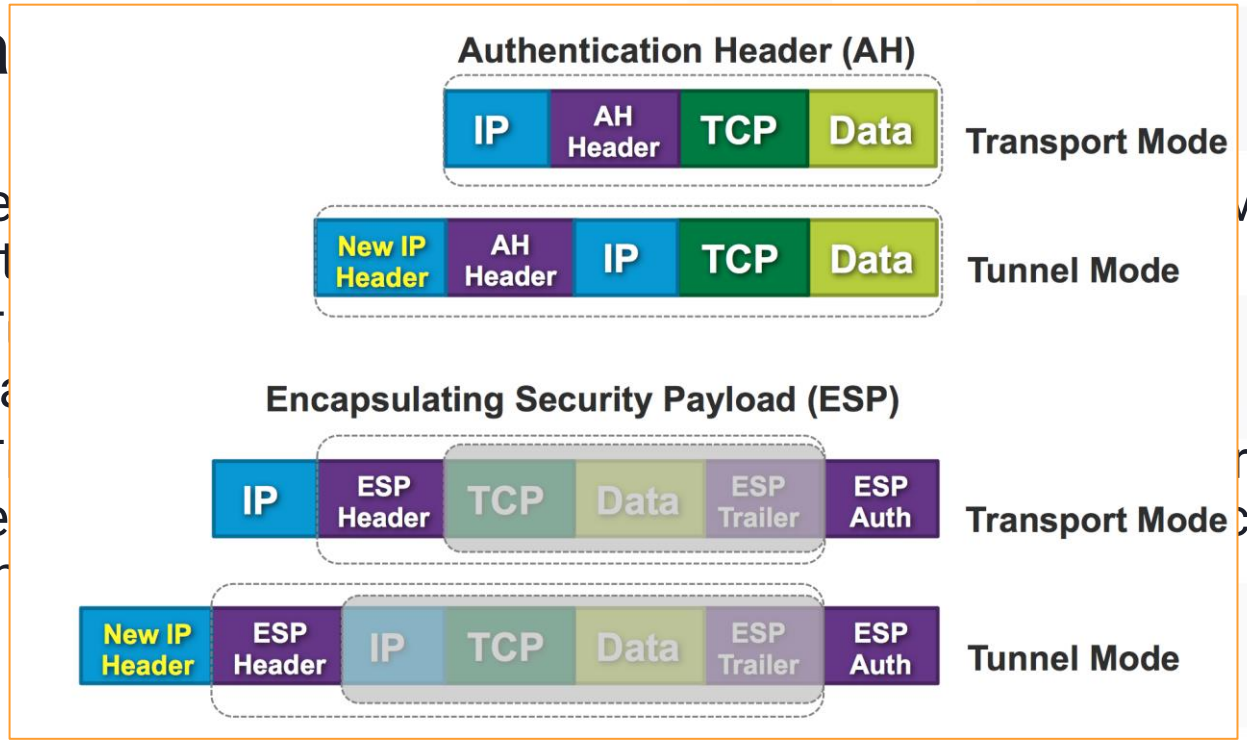
origina

heade

syster

riginal

ceiving



LECTURE

Implementing Cryptography

IPSec

IKE

- IPsec can use a variety of encryption algorithms, such as MD5 or SHA-1 for integrity, and triple DES or AES for confidentiality
- The algorithm selection process is negotiated by the Internet Key Exchange
- Two sides of an IPsec tunnel will typically use IKE to negotiate to the highest and fastest level of security, selecting AES over single DES for confidentiality if both sides support AES, for example

LECTURE

Implementing Cryptography

SSL and TLS

- SSL authenticates and provides confidentiality to Web traffic
- Transport Layer Security (TLS) is the successor to SSL
- SSL and TLS are commonly used as part of HTTPS (Hypertext Transfer Protocol Secure)
- When you connect to a Web site such as https://www.isc2.org/, the data is encrypted. This is true even if you have not preshared a key: the data is encrypted out of the gate. This is done via asymmetric encryption: your browser downloads the digital certificate of www.isc2.org, which includes the site's public key, signed by the Certificate Authority's private key. If your browser trusts the CA (such as Verisign), then this signature authenticates the site: you know its isc2.org and not a rogue site. Your browser then uses that public key to securely exchange a symmetric session key. The private key is stored on the isc2.org Web server, which allows it to decrypt anything encrypted with the public key. The symmetric key is then used to encrypt the rest of the session.
- SSL was developed for the Netscape Web browser in the 1990s. SSL 2.0 was the first released version; SSL 3.0 fixed a number of security issues with version 2.

LECTURE

Implementing Cryptography

SSL and TLS

- SSL authenticates and provides confidentiality to Web traffic
- Transport Layer Security (TLS) is the successor to SSL
- SSL a
  Secur
- When
  encry
  out o
  the di
  by the
  Verisi
  a rogu
  symmetric session key. The private key is stored on the isc2.org Web server, which allows it to decrypt anything encrypted with the public key. The symmetric key is then used to encrypt the rest of the session.
- SSL was developed for the Netscape Web browser in the 1990s. SSL 2.0 was the first released version; SSL 3.0 fixed a number of security issues with version 2.

Secure Sockets Layer (SSL) is deprecated.

TLS 1.3 is current, released in RFC 8446 (August 2018). There were many security changes and updates from TLS 1.2.

LECTURE

Implementing Cryptography

PGP

- Pretty Good Privacy – **Asymmetric** Encryption
- Released by Phil Zimmerman in 1991
- Uses a **Web of trust model** to authenticate digital certificates, instead of relying on a central certificate authority (CA) - If you trust that my digital certificate authenticates my identity, the Web of trust means you trust all the digital certificates that I trust.

LECTURE

Implementing Cryptography

S/MIME

- MIME (Multipurpose Internet Mail Extensions)
- S/MIME (Secure/MIME) leverages PKI to encrypt and authenticate MIME-encoded email
- Encryption may be done by the client or client's email server (called an S/MIME gateway)

LECTURE

Implementing Cryptography

Escrowed Encryption

- Takes a private key and divides it into two or more parts
- The parts are held in escrow by different trusted third-party organizations, which will only release their portion of the key with proper authorization, such as a court order
- Balance between an individual's privacy, and the needs of law enforcement

LECTURE

Implementing Cryptography

OOPS!

Clipper Chip

- The name of the technology used in the Escrowed Encryption Standard (EES)
- Announced in 1993 by the United States government to deploy escrowed encryption in telecommunications devices
- Created a media firestorm, and was abandoned by 1996
- Used the Skipjack algorithm, a symmetric cipher that uses an 80-bit key, an algorithm that was originally classified as secret
- Skipjack was later declassified in 1998

LECTURE

Implementing Cryptography

Steganography

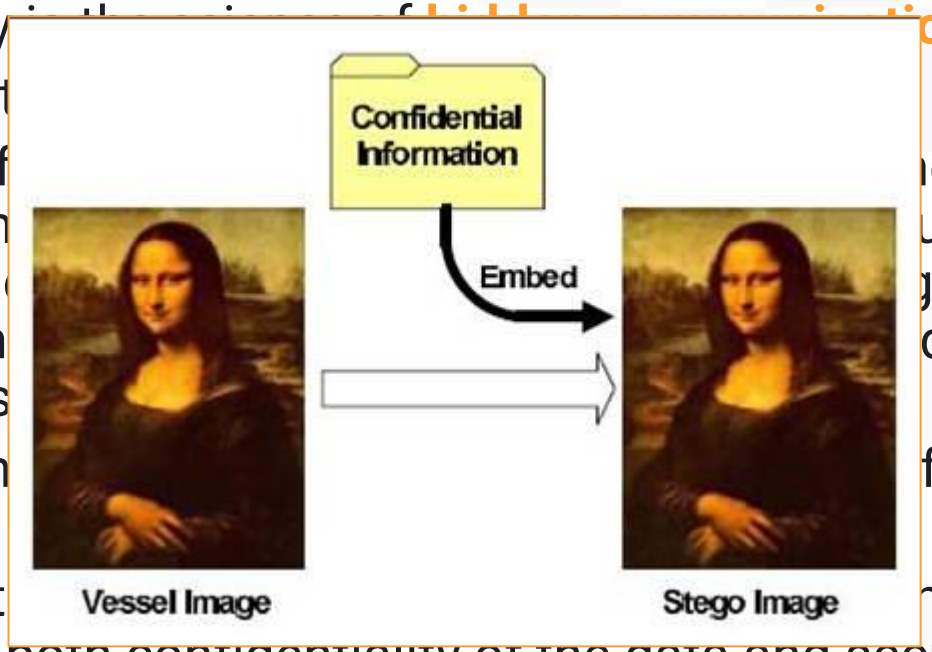
- Steganography is the science of **hidden communication**
- Hides the fact that communication is taking place
- The first use of steganography was documented by the ancient Greek historian Herodotus in the Histories of Herodotus. Herodotus described shaving a slave's head, tattooing instructions on it, waiting for the hair to grow back, and sending the slave across enemy lines.
- Modern steganography hides information inside data files, such as images
- Messages that are hidden via steganography are often encrypted first, providing both confidentiality of the data and secrecy of the communication

LECTURE

Implementing Cryptography

Steganography

- Steganography
- Hides the fact t
- The first use of
- Modern stegan
- Messages that



LECTURE

Implementing Cryptography

Digital Watermarks

- Digital Watermarks encode data into a file
- The watermark may be hidden, using steganography
- Good story from the book…

An example of real-world digital watermark use is the watermarking of DVDs by the Academy of Motion Picture Arts and Sciences. Members of the academy (who decide the recipients of Oscar awards) receive DVD “screeners” of nominated films. The films are often still being shown in movie theaters and not yet available on DVD (publicly). When the DVD system was first implemented, illegal copies of the screeners would appear on peer-to-peer filesharing networks. These copies were “ripped” (digitally copied) from the screeners. In response, the Academy of Motion Picture Arts and Sciences began watermarking each screener. Each DVD is customized for the recipient: every frame of every DVD contains a hidden watermark, tying the DVD to the recipient. Should the DVD appear on a P2P network, the academy can track the copy down the source DVD (and member who received it). In 2007, Salvador Nunez Jr. was arrested for posting the movie Flushed Away online, copied from an academy screener. Investigators used the watermark to track the copy to a screener received by his sister, who was a member of the academy.

LECTURE

Thank God!

We're done with Encryption!

Now onto Physical Security…

Remember our definition of information security:

*The application of administrative, **physical**, and technical controls to protect the confidentiality, integrity, and availability of information.*

LECTURE

Physical Security – Unique Terms and Definitions

- **Mantrap** - A preventive physical control with two doors. Each door requires a separate form of authentication to open
- **Bollard**—A post designed to stop a car, typically deployed in front of building entrances
- **Smart card**—A physical access control device containing an integrated circuit
- **Tailgating**—Following an authorized person into a building without providing credentials

A card with a high IQ?

LECTURE

Physical Security

Introduction

- Physical assets: people, buildings, systems, and data
- CISSP® exam considers **human safety** as the most critical concern of this domain - trumps all other concerns
- Physical security protects against threats such as unauthorized access and disasters, both man-made and natural

LECTURE

Physical Security

Perimeter Defenses

- Help prevent, detect, and correct unauthorized physical access
- Should employ defense-in-depth
- Fences, doors, walls, locks, etc.

Fences

- May range from deterrents (such as 3-foot/1 meter-tall fencing) to preventive devices (8-foot/2.4 meter)
- Should be designed to steer ingress and egress to controlled points, such as exterior doors and gates

LECTURE

Physical Security

Gates

- Range in strength from ornamental (a class I gate designed to deter access) to a class IV gate designed to prevent a car from crashing through (such as gates at airports and prisons)
- ASTM International's “ASTM F2200” Standard Specification for Automated Vehicular Gate Construction at http://www.astm.org/Standards/F2200.htm
- Types of Vehicle Gates:
    - **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)**
- Gates should be placed at controlled points at the perimeter - Secure sites use fences and topography to steer traffic to these points.

LECTURE

Physical Security

Gates

- Range in strength from ornamental (a class I gate designed to deter access) to a cla hing through (such a
- ASTM Internati r Automated Veh http://www.ast
- Types of Vehic
  - Class I
  - Class I
  - Class I eeler trucks)
  - Class I
- Gates should b Secure sites use fence s.

LECTURE

Physical Security

Bollards

- A traffic bollard is a strong post designed to stop a car
- Term derives from the short/strong posts (called mooring bollards) used to tie ships to piers when docked
- Often installed in front of convenience stores, to prevent a confused driver who mixes up the accelerator and brake from driving into the store.
- Used in secure facilities to prevent cars from entering (whether intentionally or not)
- Can use large concrete planters for the same effect
- Usually placed in front of physically weak areas of a building, such as entryways

LECTURE

Physical Security

Bollards

- A traffic b
- Term deri
  bollards)
- Often inst
  confused
  driving int
- Used in se
  intentiona
- Can use la
- Usually pl
  such as e

LECTURE

Physical Security

Lights

- Can act as both a detective and deterrent control
- Criminals will usually favor a poorly lighted target over a more visible one
- Should be bright enough to illuminate the desired field of vision (the area being protected)
- Fresnel (pronounced fray-NELL) lights - Same type originally used in lighthouses, use Fresnel lenses to aim light in a specific direction
- Light measurement:
    - Lumen, the amount of light one candle creates
    - Footcandles; one footcandle is one lumen per square foot
    - Lux, based on the metric system, more commonly used now: one lux is one lumen per square meter.

LECTURE

Physical Security

CCTV

- Closed Circuit Television (CCTV)
- Detective device used to aid in detecting the presence of intruders in restricted areas
- Can also be used as a deterrent device/control
- CCTVs using the normal light spectrum require sufficient visibility to illuminate the field of view

Are cloud-enabled surveillance cameras considered CCTV?

LECTURE

Physical Security

CCTV

- Infrared devices can “see in the dark” by displaying heat
- Older “tube cameras” are analog devices
- Modern cameras use CCD (Charged Couple Discharge), which is digital
- Cameras have mechanical irises that act as human irises, controlling the amount of light that enters the lens by changing the size of the aperture
- Key issues include depth of field (the area that is in focus) and field of view (the entire area viewed by the camera)
- More light allows a larger depth of field because a smaller aperture places more of the image in focus
- A wide aperture (used in lower light conditions) lowers the depth of field

LECTURE

Physical Security

CCTV

- Features such as pan and tilt (moving horizontally and vertically)
- Displays may display:
    - Fixed camera view
    - Autoscan (show a given camera for a few seconds before moving to the next)
    - Multiplexing (where multiple camera feeds are fed into one display)
- Magnetic tape such as VHS is used to back up images from tube cameras
- CCD cameras use DVR (Digital Video Recorder) or NVR (Network Video Recorder) for backups
- NVR has the advantage of allowing centralized storage of all video data

LECTURE

Physical Security

CCTV

ing horizontally and vertically)

- NVR has the advantage of allowing
  video data

LECTURE

Physical Security

Locks

- Preventive physical security control
- Used on doors and windows to prevent unauthorized physical access
- May be mechanical, such as key locks or combination locks
- May be electronic - often used with smart cards or magnetic stripe cards

Key locks

- Require a physical key to unlock
- Keys may be shared or sometimes copied, which lowers the accountability of key locks
- A common type is the pin tumbler lock, which has two sets of pins: driver pins and key pins.
- The correct key makes the pins line up with the shear line, allowing the lock tumbler (plug) to turn

LECTURE

Physical Security

Key locks

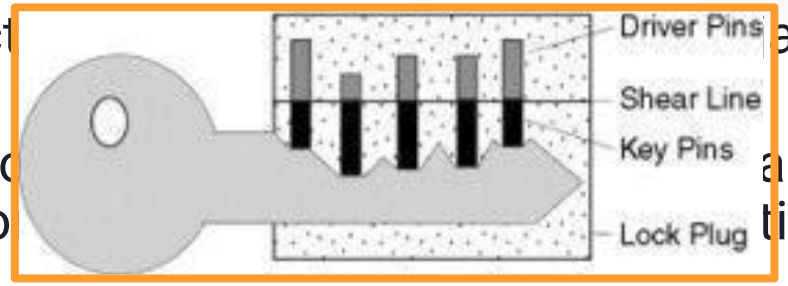
- Using an incorrect key results in misaligned pins, jamming the lock plug
- Ward or Warded locks must turn a key through channels (called wards); a “skeleton key” is designed to open varieties of warded locks
- A spring-bolt lock is a locking mechanism which “springs” in and out of the door jamb
- The door may be closed with the spring bolt exposed
- A deadbolt is rigid; the door cannot be closed when the deadbolt is unlocked
- Both spring-bolt and deadbolts extend into the strike plate in the door jamb

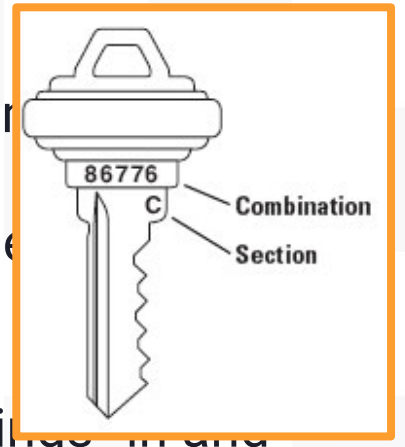
LECTURE

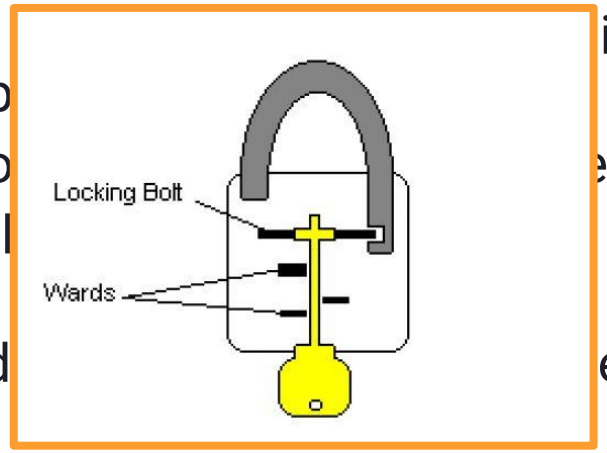
Physical Security

Key locks

- Using an incorrect
  lock plug
- Ward or Warded lo



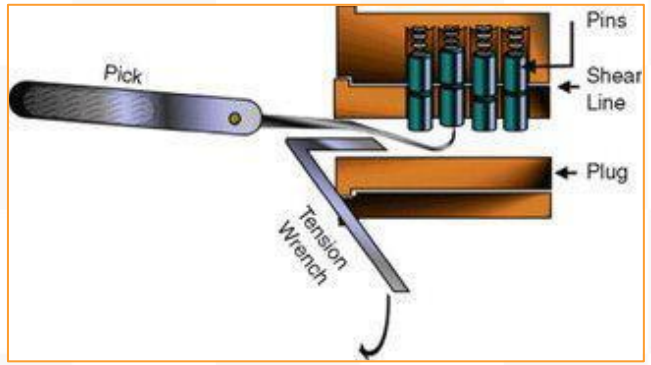




LECTURE

Physical Security

Lock Picking



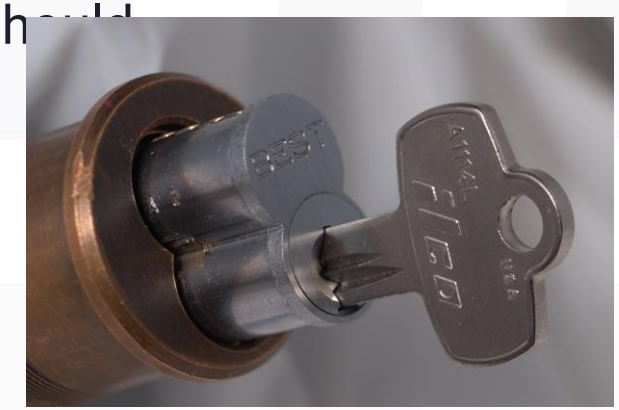
- The art of opening a lock without a key
- A set of lock picks can be used to lift the pins in a pin tumbler lock, allowing the attacker to open the lock without a key
- A technique called lock bumping uses a shaved-down key which will physically fit into the lock. The attacker inserts the shaved key and “bumps” the exposed portion (sometimes with the handle of a screwdriver). This causes the pins to jump, and the attacker quickly turns the key and opens the lock.
- All key locks can be picked or bumped: the only question is how long it will take

LECTURE

Physical Security

Master and Core Keys

- Opens any lock for a given security zone in a building
- Access to the master key should be tightly controlled
- Core keys are used to remove the lock core in interchangeable core locks (where the lock core may be easily removed and replaced with another core)
    - Once the lock core is removed, the door may often be opened with a screwdriver
    - Functional equivalent to the master key, core keys should be kept equally secure



LECTURE

Physical Security

Combination Locks

- Have dials that must be turned to specific numbers, in a specific order (alternating clockwise and counterclockwise turns) to unlock
- A **weak** form of physical access control for production environments such as data centers
- Button or keypad locks also use numeric combinations
- Limited accountability due to shared combinations
- Button or keypad locks are also vulnerable because prolonged use can cause wear on the most used buttons or keys
- Combinations may be discovered via a brute-force attack, where every possible combination is attempted
- Locks may also be compromised via shoulder surfing
- Simple locks such as pushbutton locks with limited combinations do not qualify as preventive devices; they are deterrent ONLY
- Can be used for low-security applications such as locking an employee restroom, but should not be used to protect sensitive data or assets

LECTURE

Physical Security

Smart Cards and Magnetic Stripe Cards

- A physical access control device which is often used for electronic locks, credit card purchases, or dual-factor authentication systems
- “Smart” means the card contains a computer circuit
- Smart card is also known as “Integrated Circuit Card” (ICC).
- May be “contact” or “contactless”

LECTURE

Physical Security

Smart Cards and Magnetic Stripe Cards

- Contact cards must be inserted into a smart card reader
- Contactless cards are read wirelessly
- One type of contactless card technology is Radio-Frequency Identification (RFID)
- Contain RFID tags (also called transponders) which are read by RFID transceivers
- Magnetic stripe card contains a magnetic stripe which stores information
    - Passive devices that contain no circuits
    - Sometimes called swipe cards: they are used by swiping through a card reader
- Many international credit cards are smart cards, while magnetic stripe cards are more commonly used as credit cards in the United States

LECTURE

Physical Security

Smart Cards and Magnetic Stripe Cards

- Contact cards must be inserted into a smart card reader
- Contactless cards are read
- One type of contactless car ency Identification (RFID)
- Contain RFID tags (also cal read by RFID transceivers
- Magnetic stripe card contai tores information
  - Passive devices that
  - Sometimes called sw ing through a card reade
- Many international credit ca agnetic stripe cards are more comm the United States

LECTURE

Physical Security

Smart Cards and Magnetic Stripe Cards

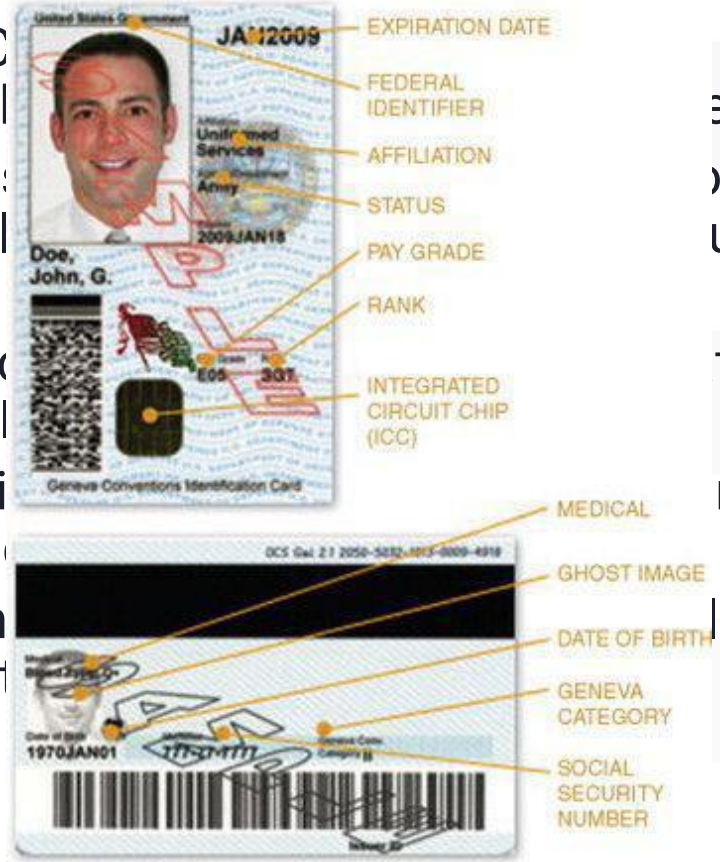
- The “Common Access Card” (CAC) is an example of a worldwide smart card deployment by the U.S. Department of Defense (DoD)
- Used for physical access control, to provide dual-factor authentication to critical systems, to digitally sign documents, and others
- CAC cards store data including cryptographic certificates as part of the DoD's Public Key Infrastructure (PKI)
- Both smart and magnetic stripe may be used in combination with electronic locks to provide physical access control
- Better accountability when compared with mechanical locks: audit data can be collected electronically

LECTURE

Physical Security

Smart Cards and Magnetic Stripe Cards

- The “Common Access C worldwide smart card deployment l ense (DoD)
- Used for physical acces: or authentication to critical uments, and others
- CAC cards store data in tes as part of the DoD's Public Key I
- Both smart and magneti nation with electronic locks to provi
- Better accountability wh l locks: audit data can be collec



LECTURE

Physical Security

Tailgating/piggybacking

- Occurs when an unauthorized person follows an authorized person into a building after the authorized person unlocks and opens the door
- Policy should forbid employees from allowing tailgating and security awareness efforts
- Attackers attempting to tailgate often combine social engineering techniques, such as carrying large boxes, increasing the chances an authorized user will “help out” by holding the door open

LECTURE

Physical Security

Tailgating/piggybacking

- Occurs when an unauthorized person follows an authorized person into a building after the authorized person unlocks and
- from a
- often
  carryi
  will "h

LECTURE

Physical Security

Mantraps and Turnstiles

- Mantraps are a preventive physical control with two doors
  - The first door must close and lock before the second door may be opened
  - Each door typically requires a separate form of authentication to open
- The intruder is trapped between the doors after entering the mantrap
- Turnstiles are designed to prevent tailgating by enforcing a “one person per authentication” rule
- Secure data centers may use floor-to-ceiling turnstiles with interlocking blades to prevent an attacker from going over or under the turnstile
- Both mantraps and turnstiles must be designed to allow safe egress in case of emergency
- No system should require authentication for egress during emergencies

LECTURE

Physical Security

Contraband Checks

- Seek to identify objects that are prohibited to enter a secure perimeter (such as an airplane)
- Secure buildings such as government or military buildings may employ contraband checks
- Often used to detect metals, weapons, or explosives
- May also be used to detect controlled substances such as illegal drugs, portable cameras or storage media

LECTURE

Physical Security

Motion Detectors and Other Perimeter Alarms

- Ultrasonic and microwave motion detectors work like “Doppler radar” used to predict the weather
    - A wave of energy is sent out, and the “echo” is returned when it bounces off an object
    - A motion detector that is 20 ft away from a wall will consistently receive an echo in the time it takes for the wave to hit the wall and bounce back to the receiver, for example. The echo will be returned more quickly when a new object (such as a person walking in range of the sensor) reflects the wave
    - Active sensors - means they actively send energy

LECTURE

Physical Security

Motion Detectors and Other Perimeter Alarms

- A photoelectric motion sensor sends a beam of light across a monitored space to a photoelectric sensor
    - The sensor alerts when the light beam is broken
    - Also an active sensor
- A passive sensor is a “read-only” device; example is a passive infrared (PIR) sensor that detects infrared energy created by body heat.

LECTURE

Physical Security

Motion Detectors and Other Perimeter Alarms

- A photoelectric motion sensor sends a beam of light across a monitored space to a photoelectric sensor
  - The sensor alerts when the light beam is broken
  - Also an active sensor
- evice
  infrar

LECTURE

Physical Security

Motion Detectors and Other Perimeter Alarms

- Perimeter alarms include magnetic door and window alarms
  - Include matched pairs of sensors on the wall, as well as window/door
  - An electrical circuit flows through the sensor pairs as long as the door or window is closed; the circuit breaks when either is opened
  - Often armed for secured areas as well as in general areas during off hours such as nights or weekends
  - Once armed, a central alarm system will alert when any door or window is opened

LECTURE

Physical Security

Motion Detectors and Other Perimeter Alarms

- Perimeter alarms include magnetic door and window alarms
  - Include matched pairs of sensors on the wall, as well as
    r
    circuit flows
    loor or windo
    s opened
    for secured
    off hours su
    a central ala
    ow is opene

LECTURE

Physical Security

Doors and Windows

- Attackers will often target the “weakest link in the chain”
- Examples of “weakest link” design include a concrete wall with a hollow-core door, or a gypsum wall with a steel door.
- Door hinges should face inward, or be otherwise protected
- Doors with internal motion sensors should never include mail slots

LECTURE

Physical Security

Doors and Windows

- Externally-facing emergency doors should be marked for emergency use only and equipped with panic bars. The use of a panic bar should trigger an alarm.
- Glass windows are structurally weak and can be dangerous when shattered. Bullet-proof or explosive-resistant glass can be used for secured areas. Wire mesh or security film can lower the danger of shattered glass and provide additional strength. Use of simple glass windows in a secure perimeter requires a compensating control such as window burglar alarms.
- Alternatives to glass windows include polycarbonate such as Lexan and acrylic such as Plexiglass. Lexan is used in race cars and airplanes for is strength and shatter resistance.

LECTURE

Physical Security

Walls, floors, and ceilings

- Walls around any internal secure perimeter such as a data center should be “slab to slab”
- Raised floors and drop ceilings can obscure where the walls truly start and stop
- Any wall protecting a secure perimeter (whether internal or external) should be strong enough to resist cutting
- Simple gypsum “sheetrock” walls can be cut open with a sharp tool such as a carpet knife, and should not be used for secure perimeters
- Walls should have an appropriate fire rating (the amount of time required to fail due to a fire)
- The National Fire Protection Agency (NFPA) 75: Standard for the Protection of Information Technology Equipment states “The computer room shall be separated from other occupancies within the building by fire-resistant rated walls, floor, and ceiling constructed of noncombustible or limited combustible materials. The fire-resistant rating shall be commensurate with the exposure, but not less than one hour.”

LECTURE

Physical Security

Guards

- A dynamic control
- May aid in inspection of access credentials, monitor CCTVs, monitor environmental controls, respond to incidents, act as a deterrent (all things being equal, criminals are more likely to target an unguarded building over a guarded building), and more
- Professional guards have attended advanced training and/or schooling; amateur guards (sometimes derogatively called “Mall Cops”) have not
- Term “pseudo guard” means an unarmed security guard
- Guard's orders should be complete and clear
- Guards are often attacked via social engineering, so this threat should be directly addressed via security awareness and training.

LECTURE

Physical Security

Dogs

- Often used in controlled areas, such as between the exterior building wall and a perimeter fence
- Primarily serve as both deterrent and detective controls
- A site without dogs is more likely to be physically attacked than a site with dogs (deterrent), and dogs alert security guards through barking (detective)
- The primary drawback to using dogs as a perimeter control is legal liability

LECTURE

Physical Security

Site selection, design, and configuration

- Describes the process of building a secure facility such as a data center, from the site selection process through the final design
- The exam could pose a scenario where you are asked about any part of the site selection process, beginning with the land the data center will be built on
- Site selection is the “greenfield” process of choosing a site to construct a building or data center. A “greenfield” is an undeveloped lot of land.

LECTURE

Physical Security

Topography

- The physical shape of the land: hills, valleys, trees, etc.
- Highly secure sites such as military installations will leverage (and sometimes alter) the topography of the site as a defensive measure
- Can be used to steer ingress and egress to controlled points

Utility Reliability

- Electrical outages are among the most common of all failures and disasters
- Uninterruptible Power Supplies (UPSs) will provide protection against electrical failure for a short period (usually hours or less)
- Generators provide longer protection, but will require refueling in order to operate for extended periods.

LECTURE

Physical Security

Crime

- Local crime rates also factor into site selection
- The primary issue is employee safety: all employees have the right to a safe working environment
- Additional issues include theft of company assets

LECTURE

Physical Security

Site Design and Configuration Issues

Site design cannot compensate for poor site selection decisions

Site Marking

- Data centers are not externally marked
- Attention-avoiding details such as muted building design

The Netflix DVD service avoids site marking of its service centers, which look like nondescript warehouses in regular office parks. There are no Netflix signs or corporate logos to be seen.

Assuming a low profile avoids drawing unwanted attention to the warehouses, which adds defense-in-depth protection to the valuable contents inside. As an additional bonus, this encourages subscribers to return DVDs via postal mail (as opposed to attempting to return DVDs by dropping them off in person).

LECTURE

Physical Security

Shared Tenancy and Adjacent Buildings

- Other tenants in a building can pose security issues: they are already behind the physical security perimeter
- Their physical security controls will impact yours: a tenant's poor visitor security practices can endanger your security
- Adjacent buildings pose a similar risk
- Attackers can enter a less secure adjacent building and use that as a base to attack an adjacent building, often breaking in through a shared wall
- Many bank heists have been pulled off this way; including the theft of over $20 million dollars from British Bank of the Middle East in 1976 (the attackers blasted a hole through the shared wall of an adjacent church) http://www.dailymail.co.uk/home/moslive/article-459185/Soldiers-Fortune.html
- Another security risk associated with shared tenancy (or neighbors who are physically close) is wireless security

LECTURE

Physical Security

Shared Demarc

- demarc (the demarcation point, where the ISP's (Internet Service Provider) responsibility ends and the customer's begins)
- Most buildings have one demarc area, where all external circuits enter the building
- Should employ strong physical access control, including identifying, authenticating, and authorizing all access
- For very secure sites, construction of multiple segregated demarcs is recommended.

LECTURE

Physical Security

System Defenses

- One of the last lines of defense in a defense-in-depth strategy
- Assume an attacker has physical access to a device or media containing sensitive information

Asset Tracking

- You cannot protect your data unless you know where (and what) it is
- Data such as serial numbers and model numbers are useful in cases of loss due to theft or disaster.

Port Controls

- Computers may contain multiple “ports” which may allow copying data to or from a system
- USB drives can be small (some are smaller than a piece of chewing gum) and inexpensive and may hold dozens of gigabytes or more
- Small enough to evade perimeter contraband checks
- Ports can be physically disabled
- Ports may also be electronically locked via system policy

LECTURE

Physical Security

Drive and Tape Encryption

- Drive and tape encryption protect data at rest
- One of the few controls which will protect data after physical security has been breached
- Recommended for all mobile devices and media containing sensitive information which may physically leave a site or security zone
- Whole-disk encryption of mobile device hard drives is recommended
- Disk encryption/decryption may occur in software or hardware
- Many breach notification laws concerning Personally Identifiable Information (PII) contain exclusions for lost data that is encrypted

LECTURE

Physical Security

Media Storage and Transportation

- All sensitive backup data should be stored offsite, whether transmitted offsite via networks, or physically moved as backup media
- Sites using backup media should follow strict procedures for rotating media offsite
- Always use bonded and insured company for offsite media storage
- The company should employ secure vehicles and store media at a secure site
- Ensure that the storage site is unlikely to be impacted by the same disaster that may strike the primary site, such as a flood, earthquake, or fire
- Never use informal practices, which as storing backup media at employee's houses

LECTURE

Physical Security

Media Cleaning and Destruction

- All forms of media should be securely cleaned or destroyed before disposal to prevent object reuse
- Objects may be physical (such as paper files in manila folders) or electronic (data on a hard drive)
- Attacks range from nontechnical attacks such as dumpster diving (searching for information by rummaging through unsecured trash) to technical attacks such as recovering information from unallocated blocks on a disk drive
- All cleaning and destruction actions should follow a formal policy, and all such activity should be documented, including the serial numbers of any hard disks, type of data they contained, date of cleaning or destruction, and personnel performing these actions

LECTURE

Physical Security

Environmental Controls

- Designed to provide a safe environment for personnel and equipment
- Power, HVAC, and fire safety are considered environmental controls

Electricity

- Reliable electricity is critical for any data center
- One of the top priorities when selecting, building, and designing a site

LECTURE

Physical Security

Types of Electrical Faults

- All types of electrical faults can impact availability and integrity
- The following are common types of 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**

← Memorize

LECTURE

Physical Security

Surge Protectors, UPSs, and Generators

Provide protection against electrical failures

Surge Protectors

- Protect equipment from damage due to electrical surges
- Contain a circuit or fuse which is tripped during a power spike or surge, shorting the power or regulating it down to acceptable levels

Uninterruptible Power Supplies

- Provide temporary backup power in the event of a power outage
- May also “clean” the power, protecting against surges, spikes, and other forms of electrical faults
- Backup power is provided via batteries or fuel cells
- Provide power for a limited period of time, and can be used as a bridge to generator power; generators typically take a short period of time to start up and begin providing power

LECTURE

Physical Security

Generators

- Designed to provide power for longer periods of times than UPSs
- Will run as long as fuel is available
- Sufficient fuel should be stored onsite for the period the generator is expected to provide power
- Refueling strategies should consider a disaster's effect on fuel supply and delivery
- Generators should not be placed in areas which may flood or otherwise be impacted by weather events
- Should be tested and serviced regularly.
- http://www.cumminspower.com/www/literature/technicalpapers/PT-7006-Standby-Katrina-en.pdf

LECTURE

Physical Security

EMI

- All electricity generates magnetism, so any electrical conductor emits Electromagnetic Interference (EMI)
- Network cables that are poorly shielded or run too closely together may suffer crosstalk, where magnetism from one cable “crosses” over to another nearby cable
- Crosstalk can be mitigated via proper network cable management
- Never route power cables close to network cables

LECTURE

Physical Security

HVAC

- Keep the air at a reasonable temperature and humidity
- Operate in a closed loop, recirculating treated air (helps reduce dust and other airborne contaminants)

Positive Pressure and Drains

- All HVAC units should employ positive pressure and drainage
- Means air and water should be expelled from the building
- Untreated air should never be “inhaled” into the building, and water should drain away from the building
- A common malfunction of HVAC units is condensation of water pooling into the building, often going under raised floors where it may not be detected
    - Positive drains are designed to avoid this problem
- Location of all gas and water lines, as well as all drains, should be formally documented.

LECTURE

Physical Security

HVAC

- Keep the air at
- Operate in a clo dust and other airborne

Positive Pressure a

- All HVAC units
- Means air and
- Untreated air sh ater should drain aw
- A common mal r pooling into the buildin not be detected
  - Positiv
- Location of all gas and water lines, as well as all drains, should be formally documented.

Summary of vendor datacenter temperature recommendations

Vendor	Low (C°/F°)	High (C°/F°)	Optimal
ASHRAE[5]	18/64.4	27/80.6	-
Enviromon[6]	18/64.4	27/80.6	-
Avtech[7]	20/68	24/75	-
Cisco[8]	18/64.4	27/80.6	-
Google[9]	-	-	26.7/80
Dell[10]	24+/Upper 70 F°	26+/Lower 80 F°	
HP[11]	18/64.4	27/80.6	
IBM[12]	18/64.4	27/80.6	
ServersCheck[4]	18/64	27/80	-
Oracle[13]	21/70	23/74	22/72

LECTURE

Physical Security

Heat and Humidity

- Humidity levels of 40-55% are recommended
- A commonly recommended “set point” temperature range for a data center is 68-77 °F (20-25 °C)
    - With sufficient data center airflow, higher temperatures can be used
    - Can result in energy savings; however, the data center may heat to dangerous levels more quickly in the event of HVAC failure

Note - Many sources cite 68-72 °F (20-22 °C) as the optimum data center temperature range; in 2004, the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommended up to 77 °F/25 °C.

- (Green) As a result, the 2008 ASHRAE recommendations allow a much wider range: temperature of 18 °C (64.4 °F) to 27 °C (80.6 °F) and humidity from 25% to 60%, depending on the dew point. Higher set points require adequate airflow. Details may be found at http://tc99.ashraetcs.org

LECTURE

Physical Security

Static and Corrosion

- Sudden static discharge can cause damage from system reboots to chip or disk damage
- Static is mitigated by maintaining proper humidity, proper grounding all circuits in a proper manner, and using antistatic sprays, wrist straps, and work surfaces
- Personnel working with sensitive computer equipment such as boards, modules, or memory chips should ground themselves before performing any work.
- High humidity levels can allow the water in the air to condense onto (and into) equipment, which may lead to corrosion.
- Both static and corrosion are mitigated by maintaining proper humidity levels.

LECTURE

Physical Security

Airborne Contaminants

- Dust is a common problem: airborne dust particles can be drawn into computer enclosures, where they become trapped
- Built-up dust can cause overheating and static buildup
- CPU fans can be impeded by dust buildup, which can lead to CPU failure due to overheating
- Other contaminants can cause corrosion or damaging chemical reactions.

LECTURE

Physical Security

Heat, Flame, and Smoke Detectors

- Three methods for detecting fire
- Typically alert locally, and may also be centrally monitored by a fire alarm system
- An audible alarm and flashing lights should be used, so that both deaf and blind personnel will be aware of the alarm

Heat Detectors

- Alert when temperature exceeds an established safe baseline
- May trigger when a specific temperature is exceeded or when temperature changes at a specific rate (such as “10 °F in less than 5 minutes”)

LECTURE

Physical Security

Smoke Detectors

- Work through two primary methods: ionization and photoelectric
- Ionization-based smoke detectors contain a small radioactive source which creates a small electric charge
- Photoelectric sensors work in a similar fashion, except that they contain an LED (Light Emitting Diode) and a photoelectric sensor that generates a small charge while receiving light
- Both types of alarm alert when smoke interrupts the radioactivity or light, lowering or blocking the electric charge
- Dust should always be avoided in data centers. Small airborne dust particles can trigger smoke detectors just as smoke does, leading to false alarms.

Flame Detectors

- Detect infrared or ultraviolet light emitted in fire
- One drawback to this type of detection is that the detector usually requires line-of-site to detect the flame; smoke detectors do not have this limitation

LECTURE

Physical Security

Safety Training and Awareness

- Training provides a skill set such as learning to operate an emergency power system
- Awareness changes user behavior (“Don't let anyone follow you into the building after you swipe your access card”)

Evacuation Routes

- Evacuation routes should be prominently posted
- All personnel should be advised of the quickest evacuation route from their areas
- Guests should be advised of evacuation routes as well
- All sites should use a meeting point, where all personnel will meet in the event of emergency

LECTURE

Physical Security

Evacuation Roles and Procedures

- The two primary evacuation roles are safety warden and meeting point leader
- The safety warden ensures that all personnel safely evacuate the building in the event of an emergency or drill
- The meeting point leader assures that all personnel are accounted for at the emergency meeting point
- Special care should be given to any personnel with handicaps, which could affect egress during an emergency
- Elevators should never be used during a fire
- All sites should have mitigating controls to allow safe egress for all personnel

LECTURE

Physical Security

ABCD Fires and Suppression

- Fire suppression systems are used to extinguish fires
- Different types of fires require different suppressive agents
- Class K fires are kitchen fires, such as burning oil or grease. Wet chemicals are used to extinguish class K fires.

LECTURE

Physical Security

Know your Fire Extinguishers

Fire Classification	Type of Fire	Type of Extinguisher	Extinguisher Identification
A	Open flames/embers of ordinary combustibles: wood, cloth, paper, rubber, some plastics	Water, Dry Powder, Halon	A
B	Flammable liquids & the associated vapors, Combustible liquids or gas	Carbon Dioxide, Dry Powder, Halon	B
C	**US**: Energized electrical equipment **Europe**: Gas Fires (add foam to list in next column)	Dry Powder, Carbon Dioxide, Halon	C
D	Combustible Metals: Magnesium, titanium, Lithium, etc.	Special Agents	D

Schlumberger

A (ash) Carbon-paper,wood,coal

B (boil) Liquids-gasoline,diesel fuel

C (current) Electrical- cables, motors

D (ding) Metals- magnesium, titanium

LECTURE

Physical Security

Types of Fire Suppression Agents

- Always consult local fire code before implementing a fire suppression system
- All fire suppression agents work via four methods (sometimes in combination):
    - reducing the temperature of the fire,
    - reducing the supply of oxygen,
    - reducing the supply of fuel,
    - interfering with the chemical reaction within fire

LECTURE

Physical Security

Types of Fire Suppression Agents

Water

- Suppresses fire by lowering the temperature below the kindling point (also called the ignition point)
- Safest of all suppressive agents, and recommended for extinguishing common combustible fires such as burning paper or wood
- It is important to cut electrical power when extinguishing a fire with water to reduce the risk of electrocution

LECTURE

Physical Security

Types of Fire Suppression Agents

Soda Acid

- Old giant brass fire extinguishers
- Suppress fire by lowering temperature, soda acid also has additional suppressive properties beyond plain water: it creates foam which can float on the surface of some liquid fires, starving the oxygen supply

LECTURE

Physical Security

Types of Fire Suppress

Soda Acid

- Old giant brass fire ex
- Suppress fire by lowe
  has additional suppre
  water: it creates foam
  of some liquid fires, s

cid also
plain
surface
ly

LECTURE

Physical Security

Types of Fire Suppression Agents

Dry Powder

- Dry powder (such as sodium chloride) works by lowering temperature and smothering the fire, starving it of oxygen.
- Dry powder is primarily used to extinguish metal fires (flammable metals include sodium, magnesium, and many others)

LECTURE

Physical Security

Types of Fire Suppression Agents

CO2

- Fires may be smothered by removing the oxygen: this is how CO2 fire suppression works.
- A risk associated with CO2 is it is odorless and colorless, and our bodies will breathe it as air. By the time we begin suffocating due to lack of oxygen, it is often too late.
- CO2 is dangerous suppressive agent, which is only recommended in unstaffed areas such as electrical substations
- Any personnel entering a CO2-protected area should be trained for CO2 safety; additional safety controls (such as oxygen tanks) are usually recommended

LECTURE

Physical Security

Types of Fire Suppression Agents

Halon and Halon Substitutes

- Extinguishes fire via a chemical reaction that consumes energy and lowers the temperature of the fire
- Halon is being phased out, and a number of replacements with similar properties are now used

Montreal Accord

- Halon has ozone-depleting properties
- The 1989 Montreal Protocol (formally called the “Montreal Protocol on Substances That Deplete the Ozone Layer”) banned production and consumption of new halon in developed countries by January 1, 1994.
- Existing halon systems may be used. While new halon is not being produced, recycled halon may be used
- There are exceptions for certain critical uses, such as airplanes and submarines. See http://ozone.unep.org for more information on the Montreal Protocol.

LECTURE

Physical Security

Types of Fire Suppression Agents

Halon Replacements

Recommended replacements for halon include the following systems:

- Argon
- FE-13
- FM-200
- Inergen

FE-13 is the newest of these agents, and comparatively safe. It may be breathed in concentrations of up to 30%. Other halon replacements are typically only safe up to 10-15% concentration.

LECTURE

Physical Security

Sprinkler Systems

- All sprinkler systems should be combined with a fire alarm that alerts people to evacuate
- Safe evacuation is the primary goal of fire safety.

Wet Pipe

- Wet pipes have water right up to the sprinkler heads: the pipes are “wet.”
- The sprinkler head contains a metal (common in older sprinklers) or small glass bulb designed to melt or break at a specific temperature
- The sprinkler head opens and water flows
- Each head will open independently as the trigger temperature is exceeded.

LECTURE

Physical Security

Wet Pipe

- Bulbs come in different colors, which indicate the ceiling temperature which will trigger the bulb to burst and open the sprinkler head
- The colors used are
  - orange (135 °F/57 °C),
  - red (155 °F/68 °C),
  - yellow (175 °F/79 °C),
  - green (200 °F/93 °C),
  - blue (286 °F/141 °C)

NFPA 13: Standard for the Installation of Sprinkler Systems describes the color conventions used for these sprinkler heads. See: http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=13

LECTURE

Physical Security

Pre-Action

- Combination of wet, dry, or deluge systems, and require two separate triggers to release water
- Single interlock systems release water into the pipes when a fire alarm triggers
- The water releases once the head opens
- Double interlock systems use compressed air (same as dry pipes): the water will not fill the pipes until both the fire alarm triggers and the sprinkler head opens
- Preaction systems are used in areas such as museums, where accidental discharge would be expensive.
- Double-interlock systems are used in cold areas such as freezers to avoid frozen pipes

LECTURE

Physical Security

Portable Fire Extinguishers

- Should be marked with the type of fire they are designed to extinguish
- Should be small enough to be operated by any personnel who may need to use one
- Use the “PASS” method to extinguish a fire with a portable fire extinguisher:
  - Pull the pin
  - Aim low
  - Squeeze the pin
  - Sweep the fire

WE MADE IT THROUGH SESHUN #5!

HOLY MOLY! That was a long Domain with a lot of information!

Please try to catch up in your reading. You've got the weekend off.

- We left off on page 212 in the book.
- Monday (5/3) gets technical.
- Evan is leading next class. He's good at technicalling!

Have a great evening, talk to you Monday!