Lesson 5

Summarizing Basic Cryptographic Concepts

CompTIA.

Topic 5A

Compare and Contrast Cryptographic Ciphers

Syllabus Objectives Covered

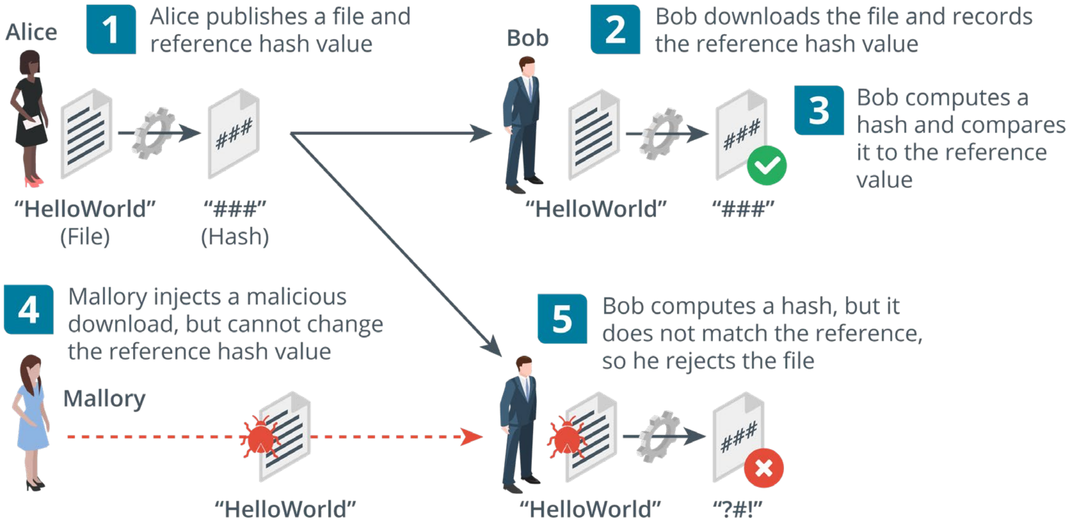
- 2.1 Explain the importance of security concepts in an enterprise environment (Hashing only)
- 2.8 Summarize the basics of cryptographic concepts

Cryptographic Concepts

- Encryption and decryption—encoding and decoding
  - Plaintext is the unencoded message
  - Ciphertext is the coded message
  - Cipher is the means of change or algorithm
  - Cryptanalysis is the art of cracking cryptographic systems
- Meet Alice and Bob (and observe Mallory, lurking)
- Hashing algorithms
- Encryption ciphers
  - Symmetric
  - Asymmetric

Hashing Algorithms

- Fixed length hash from variable string with cryptographic properties
  - One-way (plaintext cannot be recovered from the digest)
  - Anti-collision (no two plaintexts are likely to produce the same checksum)
- Used for password storage and checksums (integrity)
- Secure Hash Algorithm (SHA)
- Message Digest Algorithm (MD5)

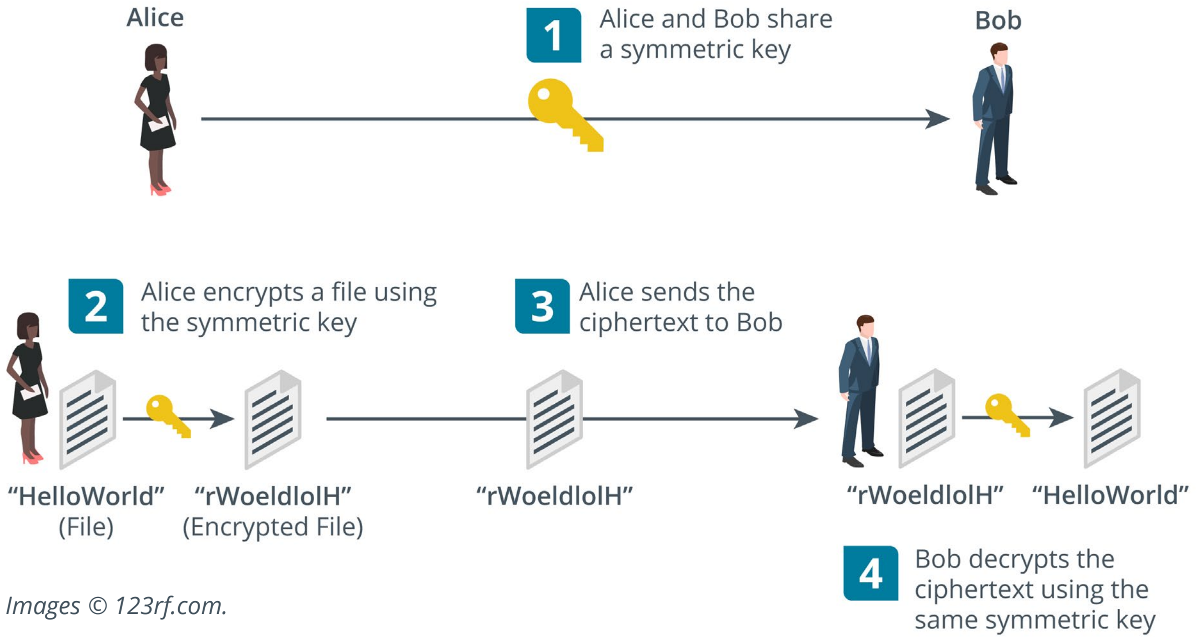

Alice
1
Alice publishes a file and reference hash value
###
"HelloWorld" (File)
"###" (Hash)
Bob
2
Bob downloads the file and records the reference hash value
3
Bob computes a hash and compares it to the reference value
###
"HelloWorld"
"###"
4
Mallory injects a malicious download, but cannot change the reference hash value
Mallory
"HelloWorld"
5
Bob computes a hash, but it does not match the reference, so he rejects the file
###
"HelloWorld"
"?#!"

Images © 123rf.com.

Encryption Ciphers and Keys

- Hashing is not encryption—the process is not reversible
- Encryption uses a reversible process based on a secret
- Process should be too complex to unravel without the secret
  - Substitution
  - Transposition
- Cannot keep the cipher/algorithm itself secret
- Key ensures ciphertext remains protected even when the operation of the cipher is known
- Protecting the key is easier than protecting the algorithm

Symmetric Encryption


Alice
1
Alice and Bob share a symmetric key
Bob
2
Alice encrypts a file using the symmetric key
3
Alice sends the ciphertext to Bob
"HelloWorld" (File)
"rWoeldlolH" (Encrypted File)
"rWoeldlolH"
"rWoeldlolH"
"HelloWorld"
4
Bob decrypts the ciphertext using the same symmetric key

Images © 123rf.com.

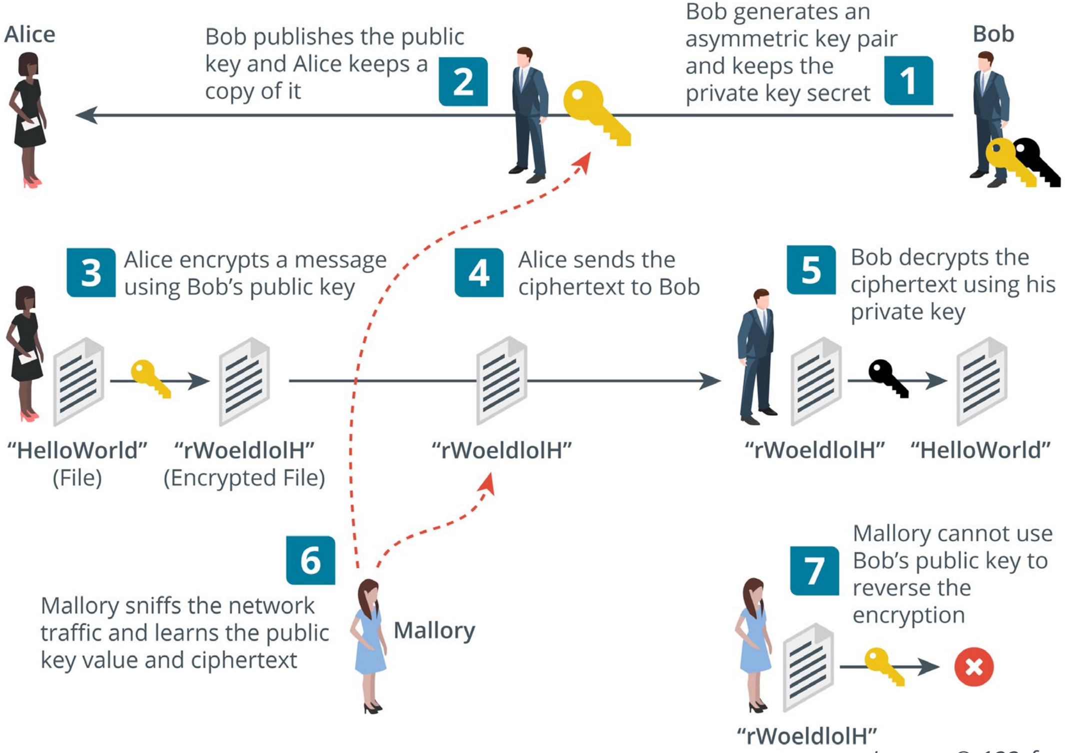
- Same secret key is used for encryption and decryption
- Fast—suitable for bulk encryption of large amounts of data
- Problem storing and distributing key securely
- Confidentiality only—sender and recipient know the same key

Stream and Block Ciphers

- Stream ciphers
  - Encrypt and decrypt each bit/byte at a time
  - Must be used with an initialization vector (IV)
- Block ciphers
  - Treat data as equal-size blocks, using padding if necessary
  - Advanced Encryption Standard (AES/AES256)
- Key length
  - Range of key values is the keyspace
  - Longer key bit length means a larger keyspace
  - Strength of key of any given length varies between ciphers

Asymmetric Encryption

- Public/private key pair
  - If the public key encrypts, only the private key can decrypt
  - If the private key encrypts, only the public key can decrypt
  - Private key cannot be derived from the public key
  - Private key must be kept secret
  - Public key is easy to distribute (anyone can have it)
- Message size is limited to key size so not suitable for large amounts of data
- Used for small amounts of authentication data


Alice
Bob
Bob publishes the public key and Alice keeps a copy of it
2
Bob generates an asymmetric key pair and keeps the private key secret
1
3
Alice encrypts a message using Bob's public key
4
Alice sends the ciphertext to Bob
5
Bob decrypts the ciphertext using his private key
"HelloWorld" (File)
"rWoeldlolH" (Encrypted File)
"rWoeldlolH"
"rWoeldlolH"
"HelloWorld"
6
Mallory sniffs the network traffic and learns the public key value and ciphertext
Mallory
7
Mallory cannot use Bob's public key to reverse the encryption
"rWoeldlolH"

Images © 123rf.com.

Public Key Cryptography Algorithms

- RSA algorithm (Rivest, Shamir, Adleman)
  - Basis of many public key cryptography schemes
  - Trapdoor function
  - Easy to calculate with the public key, but difficult to reverse without the private key
- Elliptic curve cryptography (ECC)
  - Concerns about RSA being vulnerable to cryptanalysis
  - Another type of trapdoor function
  - Can use smaller keys to obtain same security

Topic 5B

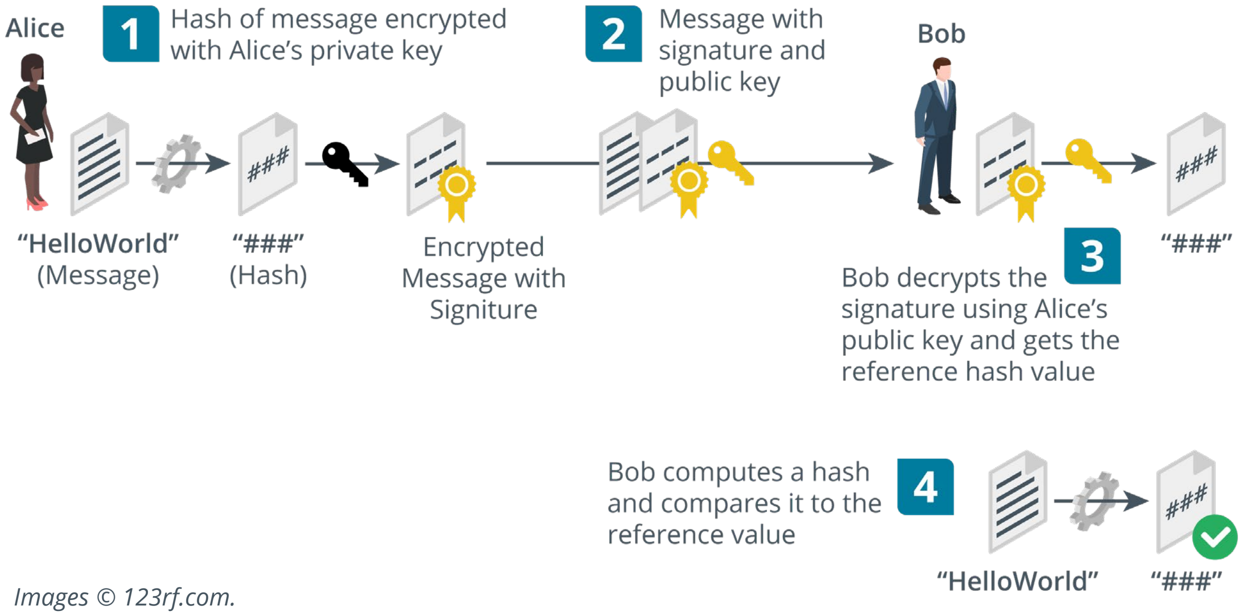
Summarize Cryptographic Modes of Operation

Syllabus Objectives Covered

- 2.8 Summarize the basics of cryptographic concepts

Digital Signatures

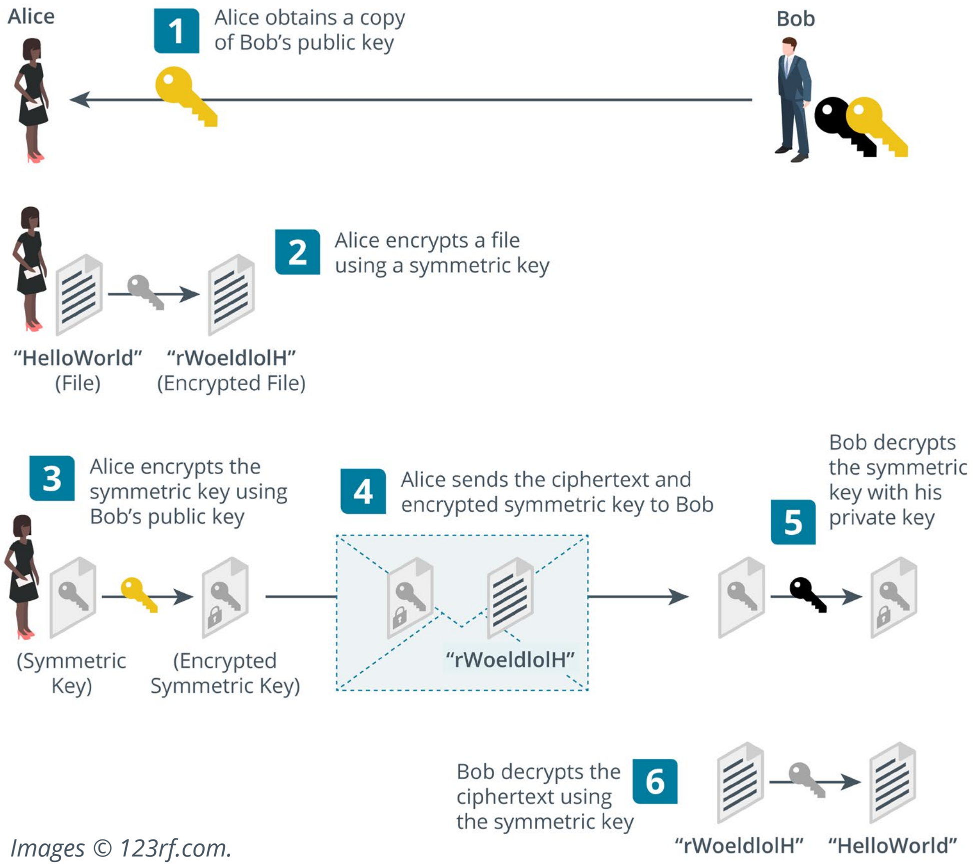
- Using public key cryptography with hashing
- Digital signatures provide integrity, authentication, non-repudiation
- RSA-based digital signatures
- Digital Signature Algorithm (DSA) with ECC cipher



Alice
1
Hash of message encrypted with Alice's private key
2
Message with signature and public key
Bob
###
"HelloWorld" (Message)
"###" (Hash)
Encrypted Message with Signiture
3
Bob decrypts the signature using Alice's public key and gets the reference hash value
"###"
Bob computes a hash and compares it to the reference value
4
"HelloWorld"
"###"

Images © 123rf.com.

Digital Envelopes and Key Exchange



Alice

1 Alice obtains a copy of Bob's public key

Bob

2 Alice encrypts a file using a symmetric key

"HelloWorld" (File)

"rWoeldlolH" (Encrypted File)

3 Alice encrypts the symmetric key using Bob's public key

4 Alice sends the ciphertext and encrypted symmetric key to Bob

Bob decrypts the symmetric key with his private key 5

(Symmetric Key)

(Encrypted Symmetric Key)

"rWoeldlolH"

Bob decrypts the ciphertext using the symmetric key 6

"rWoeldlolH"

"HelloWorld"

Images © 123rf.com.

Digital Certificates

- Wrapper for a public key to associate it with a digital identity
- Identity assertion is validated by a certificate authority (CA) by signing the certificate
- Both parties must trust the CA
- Referred to as public key infrastructure (PKI)

Perfect Forward Secrecy

- RSA key exchange decrypts the session key using the server private key
- The private key stored on the server may be compromised in the future
- If key is compromised, previously captured transmissions could be deciphered
- Perfect forward secrecy (PFS) mitigates this issue
- Uses Diffie-Hellman key agreement protocols
- Allows two parties to derive the same secret value that an eavesdropper cannot guess

Cipher Suites and Modes of Operation

- Cipher suite
  - Signature algorithm—proves messages were created by the server (authentication and integrity)
  - Key exchange/agreement algorithm—allows client and server to agree session keys
  - Bulk encryption cipher—uses the session key to keep the data confidential
- Modes of operation
  - Use symmetric block cipher with arbitrary length network data
  - Cipher Block Chaining (CBC)
    - Combines blocks and an initialization vector (IV) using XOR operation
    - Data must be a multiple of block size so requires padding for last block
  - Counter mode
    - Generates keystream with IV and counter
    - Does not require block padding

Authenticated Modes of Operation

- Unauthenticated encryption
  - Secret key encryption cannot prove integrity
  - Makes cryptographic system vulnerable to insertion and modification attacks
- Authenticated encryption
  - Message authentication code (MAC)
  - Create a hash from combination of the message and a shared secret
  - Implementations vulnerable to padding oracle attacks
- Authenticated encryption with additional data (AEAD)
  - Counter modes or stream ciphers that do not use padding
  - Associates message with context to prevent replay

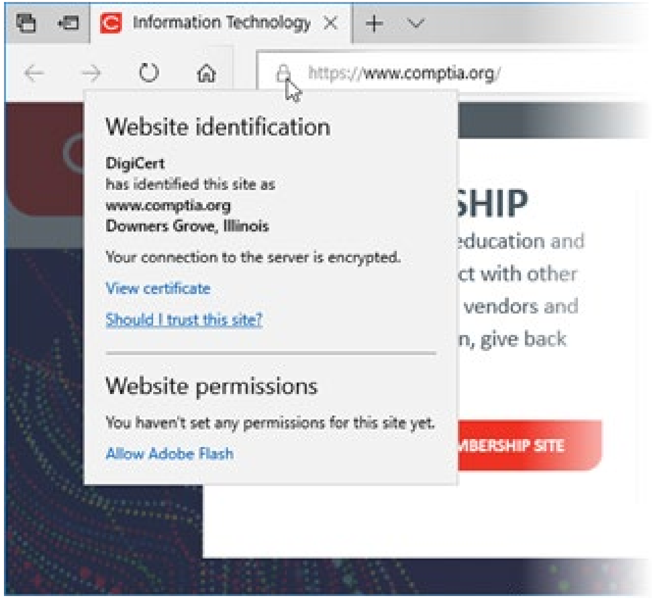
Topic 5C

Summarize Cryptographic Use Cases and Weaknesses

Syllabus Objectives Covered

- 1.2 Given a scenario, analyze potential indicators to determine the type of attack
- 2.8 Summarize the basics of cryptographic concepts

Cryptography for Authentication and Non-repudiation



Website identification

DigiCert
has identified this site as
www.comptia.org
Downers Grove, Illinois

Your connection to the server is encrypted.

View certificate

Should I trust this site?

Website permissions

You haven't set any permissions for this site yet.

Allow Adobe Flash

Screenshot used with permission from Microsoft.

- Cryptographic primitives versus cryptographic systems
- Authentication and access control
  - Assuming the private key is secure, an encrypted token could only have been created by the key holder
- Non-repudiation
  - Sender cannot deny (repudiate) the message as only she/he could have created it

Cryptography Supporting Confidentiality

- Hybrid encryption
  - Public key cryptography is only efficient with small amounts of data
  - Symmetric encryption makes key distribution difficult
  - Symmetric key is used for bulk encryption and protected by public key cryptography
- File encryption
  - Private key encrypts the symmetric key
  - Use of the key is locked to a user account credential
- Transport encryption
  - Session key exchange/agreement

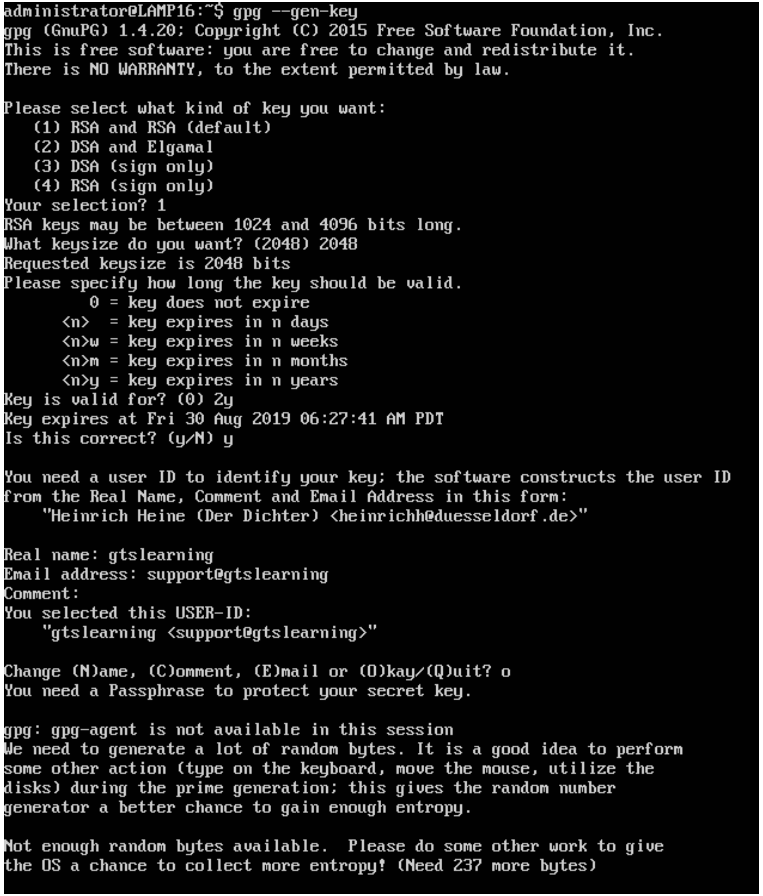
Cryptography Supporting Integrity and Resiliency

- Integrity
  - Using hash functions and message authentication codes to validate messages
- Resiliency
  - Using cryptography to ensure authentication and integrity of control messages
- Obfuscation
  - Make something hard to understand
  - Encryption can perform this function, but it is very hard to secure an embedded key
  - White box cryptography

Cryptographic Performance Limitations

- Limitations
  - Speed—Amount of data/number of operations per second
  - Time/latency—Delay in completing an operation
  - Size—Key size increases security but also CPU/memory requirements
  - Computational overhead—Complexity of cryptographic implementation or cipher
- Resource-constrained environments
  - Low-power devices
    - Battery-powered systems
    - Contactless smart cards
  - Low latency
    - Delay-sensitive communications protocols/implementations

Cryptographic Security Limitations



```
administrator@LAMP16:~$ gpg --gen-key
gpg (GnuPG) 1.4.20; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 2y
Key expires at Fri 30 Aug 2019 06:27:41 AM PDT
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: gtslearning
Email address: support@gtslearning
Comment:
You selected this USER-ID:
    "gtslearning <support@gtslearning>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? o
You need a Passphrase to protect your secret key.

gpg: gpg-agent is not available in this session
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.

Not enough random bytes available.  Please do some other work to give
the OS a chance to collect more entropy! (Need 237 more bytes)
```

- Entropy
  - Checksums and ciphertext must reduce order (high entropy)
  - Weak ciphers and weak keys
  - Weak implementations
  - Weak randomness
- Predictability and reuse
  - Nonce
  - Initialization vector (IV)
  - Salt

Longevity and Cryptographic Attacks

- How secure are current algorithms?
- How long must a ciphertext be resistant to attacks?

Man-in-the-Middle and Downgrade Attacks

- Man-in-the-Middle (MitM)
    - Interferes with the public key presented to the client
- Downgrade attack
    - Forces server into using weak protocol versions and ciphers

Key Stretching and Salting

- User-generated data is low entropy
- Key stretching
  - Use additional rounds to strengthen keys
  - Makes attacker do more work so slows down brute force
- Salting
  - Add a random value to each password when hashing it for storage
  - Prevents use of pre-computed hash tables

Collisions and the Birthday Attack

- Exploit collisions to forge a signature
- Math of birthday paradox shows that this might be easier than expected
- Chosen prefix collision attacks

Topic 5D

Summarize Other Cryptographic Technologies

Syllabus Objectives Covered

- 2.8 Summarize the basics of cryptographic concepts

Quantum

- Quantum computing
  - Quantum bit (qubits), superpositions, entanglement and collapse
  - Quantum computers can keep track of a lot of state data at the same time
- Communications
  - Tamper-evident key distribution
- Post-quantum
  - Quantum-based cryptanalysis
  - Post-quantum cryptography (replacements for the current algorithms)
- Lightweight cryptography

Homomorphic Encryption

- Supports data analytics functions while preserving confidentiality and privacy

Blockchain

- Expanding list of transactional records (blocks)
- Each block is linked by hashing
- Public ledger
  - Ledger of transactions performed on a digital asset
  - Peer-to-peer so transactions are public
  - Transactions cannot be deleted or reversed
- Widely used for cryptocurrencies
- Potential uses for financial transactions, online voting systems, identity management systems, notarization, data storage, ...

Steganography

- Concealing messages within a covertext
- Often uses file data that can be manipulated without introducing obvious artifacts
    - Image
    - Audio
    - Video
- Covert channels

Lesson 5

Summary