SLIIT

Discover Your Future

IE2022 – Introduction to Cyber Security

Lecture - 06

Cryptography II- Hash Functions and Key Management

Mr. Amila Senarathne

Cryptographic Hash Functions and Key Management

- Reading Assignment
  - CCNA Security Curriculum, Chapter 7: Cryptographic Systems

- Supplementary text
  - W. Stallings and L. Brown, “Computer Security, Principles and Practice, 2nd edition, Pearson, 2012, Chapter 2 :Cryptographic Tools.

Topics to be discussed

- Cryptographic Hash Function
  - Cryptographic Hash Function Properties
  - MD5 and SHA
- Keyed-Hash Message Authentication Code (HMAC)
- Characteristics of Key Management

Cryptology - The Secret Is in the Keys

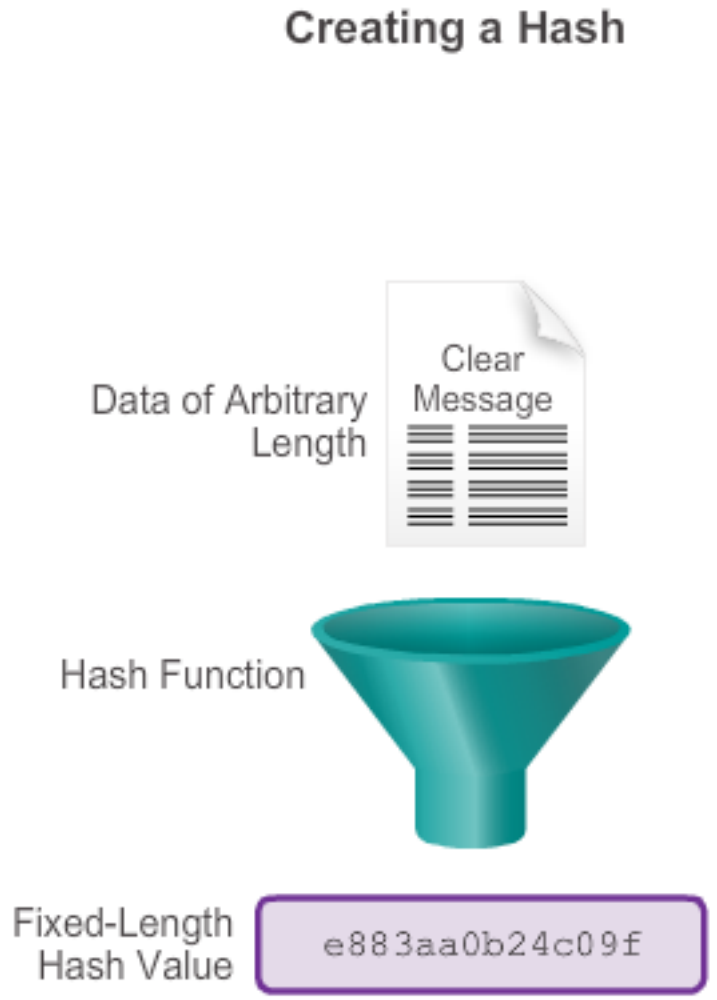
- Authentication, integrity, and data confidentiality are implemented in many ways using various protocols and algorithms. Choice depends on the security level required in the security policy.

	Integrity	Authentication	Confidentiality
Common cryptographic hashes, protocols, and algorithms	MD5 (weaker) SHA (stronger)	HMAC-MD5 HMAC-SHA-1 RSA and DSA	DES (weaker) 3DES AES (stronger)

BASIC INTEGRITY AND AUTHENTICITY

Cryptographic Hash Functions

- A hash function takes binary data (message), and produces a condensed representation, called a hash. The hash is also commonly called a Hash value, Message digest, or Digital fingerprint.
- Hashing is based on a one-way mathematical function that is relatively easy to compute, but significantly harder to reverse.
- Hashing is designed to verify and ensure:
  - Data integrity
  - Authentication

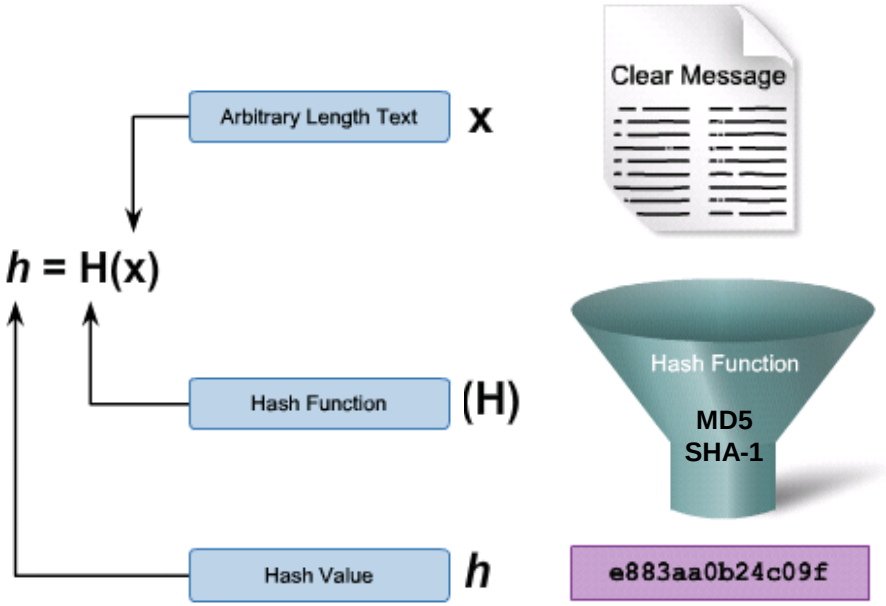


Cryptographic Hash Functions

- Cryptographic hash function is applied in many different situations:
  - To provide proof of authenticity when it is used with a symmetric secret authentication key, such as IP Security (IPsec) or routing protocol authentication.
  - To provide authentication by generating one-time and one-way responses to challenges in authentication protocols, such as the PPP CHAP.
  - To provide a message integrity check proof, such as those accepted when accessing a secure site using a browser.
  - To confirm that a downloaded file (e.g., Cisco IOS images) has not been altered.

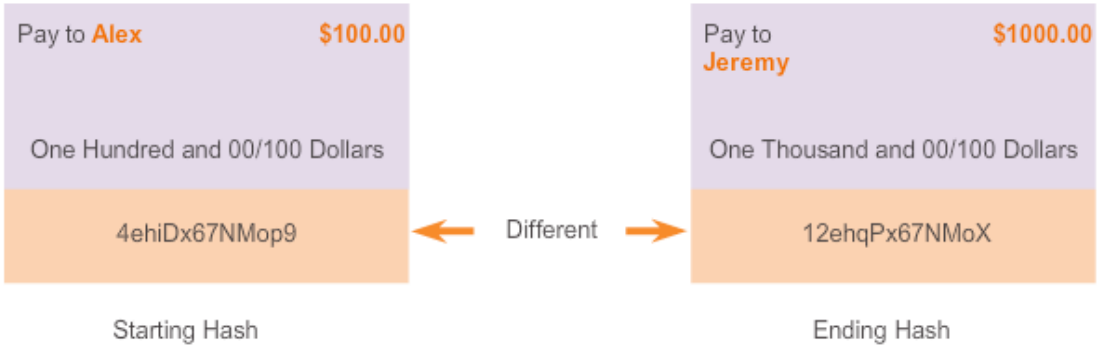
Cryptographic Hash Function Properties

- Take an arbitrarily length of clear text data to be hashed.
- Put it through a hash function.
- It produces a fixed length message digest (hash value).
- H(x) is:
  - Relatively easy to computer for any given x.
  - One way and not reversible.
- If a hash function is hard to invert, it is considered a one-way hash.



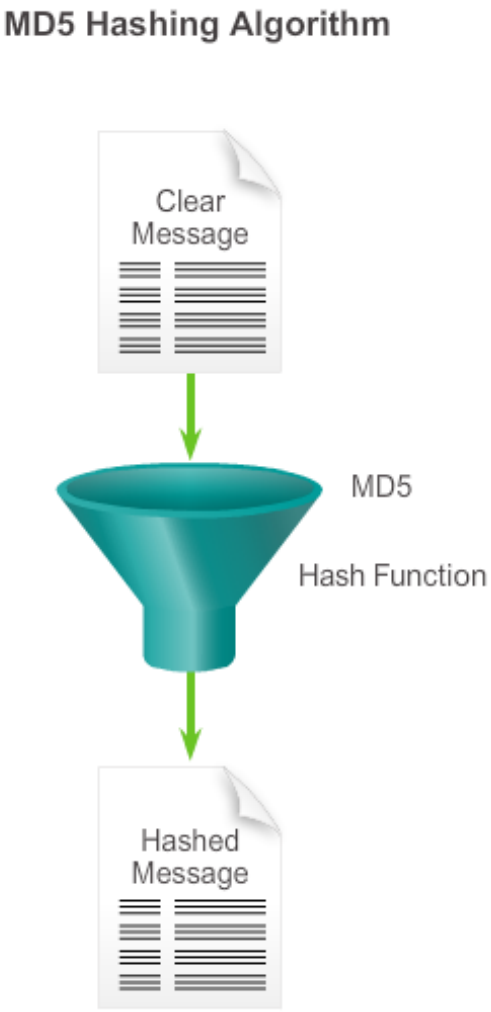
Well-Known Hash Functions

- Hash functions are helpful when ensuring data is not changed accidentally, such as by a communication error.
- Hash functions cannot be used to guard against deliberate changes.
- There is no unique identifying information from the sender in the hashing procedure, so anyone can compute a hash for any data, as long as they have the correct hash function.
- Hashing is vulnerable to man-in-the-middle attacks and does not provide security to transmitted data.
- Two well-known hash functions are:
  - MD5 with 128-bit digests
  - SHA-256 with 256-bit digests



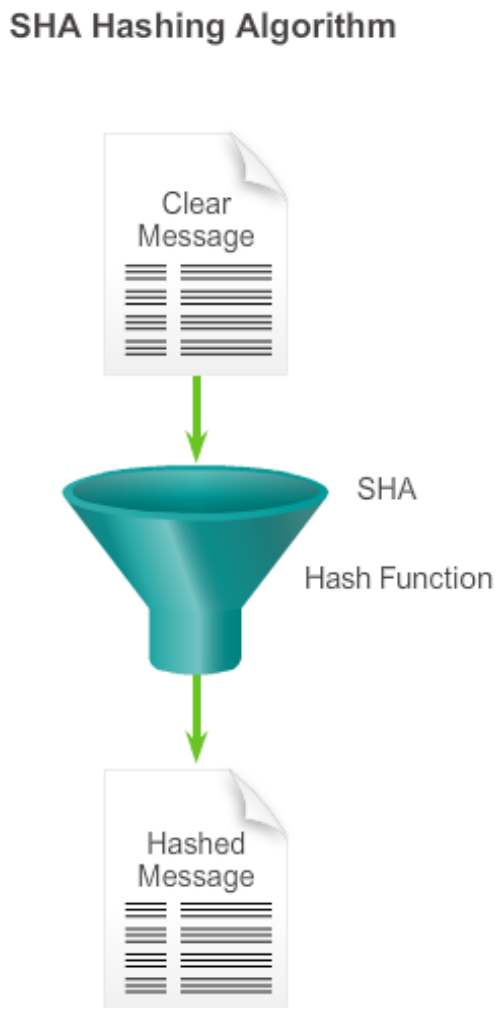
Message Digest 5 Algorithm

- MD5 algorithm is a hashing algorithm that was developed by Ron Rivest.
- Used in a variety of Internet applications today.
- A one-way function that makes it easy to compute a hash from the given input data, but makes it unfeasible to compute input data given only a hash value.



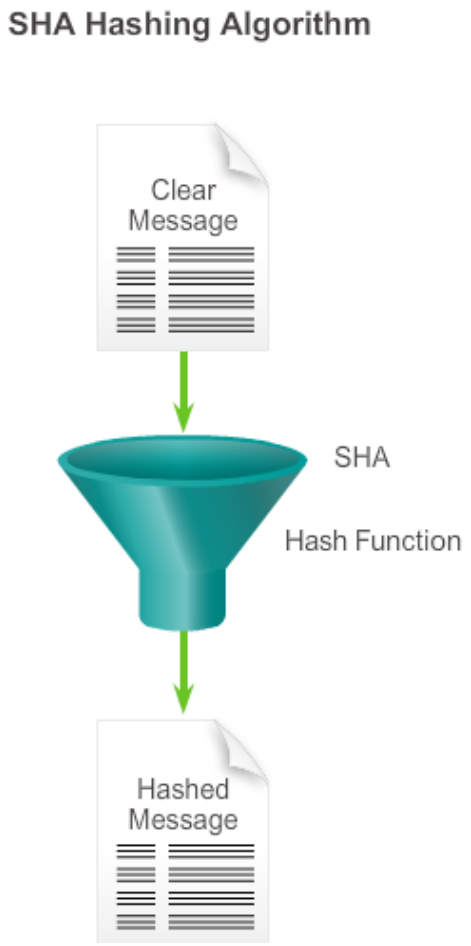
Secure Hash Algorithm

- U.S. National Institute of Standards and Technology (NIST) developed SHA, the algorithm specified in the Secure Hash Standard (SHS).
- SHA-1, published in 1994, corrected an unpublished flaw in SHA.
- SHA design is very similar to the MD4 and MD5 hash functions that Ron Rivest developed.



Secure Hash Algorithm

- SHA-1 algorithm takes a message of less than 2^64 bits in length and produces a 160-bit message digest.
- Slightly slower than MD5, but the larger message digest makes it more secure against brute-force collision and inversion attacks.
- NIST published four additional hash functions in the SHA family, each with longer digests:
  - SHA-224 (224 bit)
  - SHA-256 (256 bit)
  - SHA-384 (384 bit)
  - SHA-512 (512 bit)



MD5 Versus SHA-1

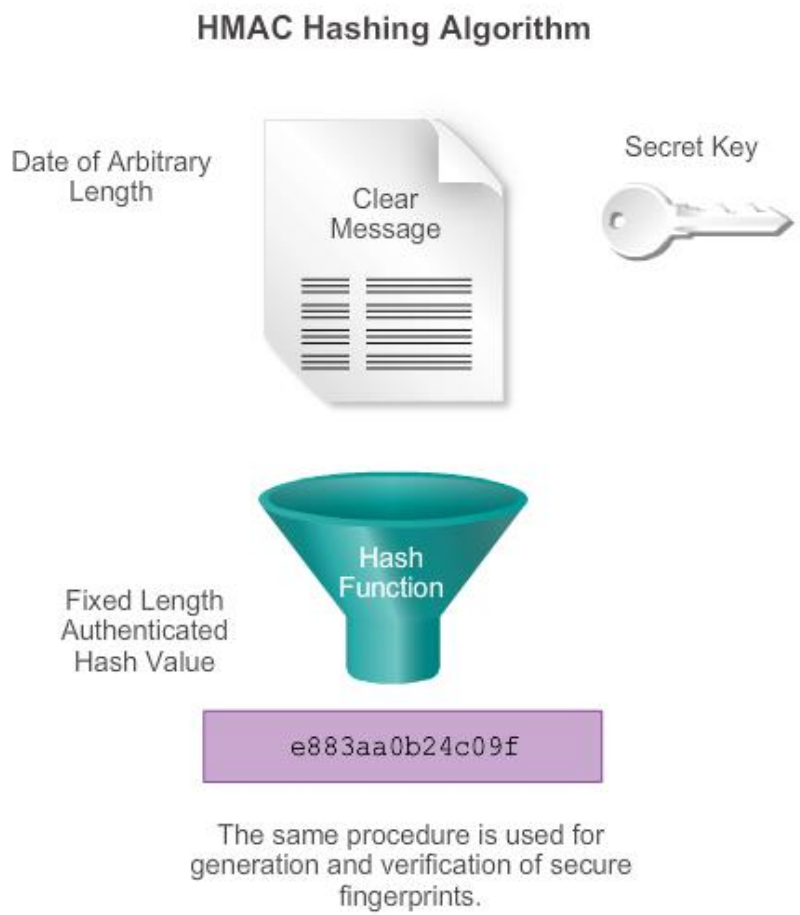
MD5	SHA-1
Based on MD4	Based on MD4
Computation involves 64 steps	Computation involves 80 steps
Algorithm must process a 128-bit buffer	Algorithm must process a 160-bit buffer
Faster	Slower
Less Secure	More secure

Keyed-Hash Message Authentication Code

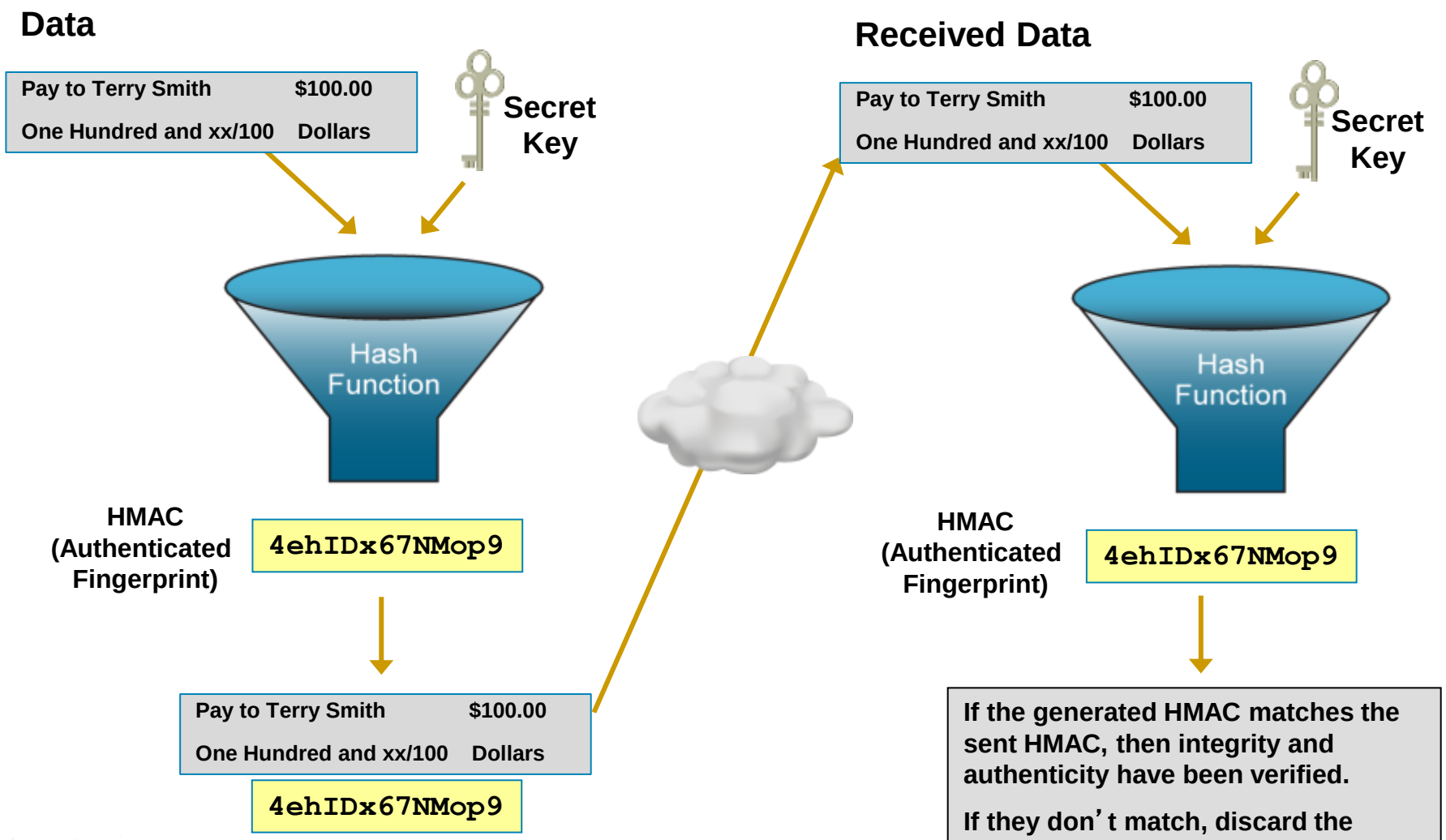
- HMAC (or KHMAC) is a message authentication code (MAC) that is calculated using a hash function and a secret key.
  - HMACs use an additional secret key as input to the hash function adding authentication to integrity assurance.
  - Hash functions are the basis of the protection mechanism of HMACs.
  - The output of the hash function now depends on the input data and the secret key.
- Authenticity is guaranteed, because only the sender and the receiver know the secret key.
  - Only they can compute the digest of an HMAC function.
  - This characteristic defeats man-in-the-middle attacks and provides authentication of the data origin.

Keyed-Hash Message Authentication Code

- The cryptographic strength of the HMAC depends on the:
  - Cryptographic strength of the underlying hash function.
  - Size and quality of the key.
  - Size of the hash output length in bits.
- Cisco technologies use two well-known HMAC functions:
  - Keyed MD5 or HMAC-MD5 is based on the MD5 hashing algorithm.
  - Keyed SHA-1 or HMAC-SHA-1 is based on the SHA-1 hashing algorithm.



HMAC Operation



Characteristics of Key Management

- Often considered the most difficult part of designing a cryptosystem.
- There are several essential characteristics of key management to consider:
  - Key generation
  - Key verification
  - Key storage
  - Key exchange
  - Key revocation and destruction

Characteristics of Key Management

- Key Generation
  - Caesar chose the key of his cipher and the Sender/Receiver chose a shared secret key for the Vigenère cipher.
  - Modern cryptographic system key generation is usually automated.
- Key Verification
  - Almost all cryptographic algorithms have some weak keys that should not be used (e.g., Caesar cipher ROT 0 or ROT 25).
  - With the help of key verification procedures, these keys can be regenerated if they occur.
- Key Storage - Modern cryptographic system store keys in memory.

Characteristics of Key Management

- Key Exchange
  - Key management procedures should provide a secure key exchange mechanism over an untrusted medium.
- Key Revocation and Destruction
  - Revocation notifies all interested parties that a certain key has been compromised and should no longer be used.
  - Destruction erases old keys in a manner that prevents malicious attackers from recovering them.
- Two terms that are used to describe keys are:
  - Key size - The measure in bits; also called the key length.
  - Keyspace - This is the number of possibilities that can be generated by a specific key length.

Characteristics of Key Management

- The key length is the measure in bits and the keyspace is the number of possibilities that can be generated by a specific key length.
- As key lengths increase, keyspace increases exponentially:
  - 2^2 key = a keyspace of 4
  - 2^3 key = a keyspace of 8
  - 2^4 key = a keyspace of 16
  - 2^{40} key = a keyspace of 1,099,511,627,776

Key Management - The Keyspace

- Adding one bit to a key doubles the keyspace.
- For each bit added to the DES key, the attacker would require twice the amount of time to search the keyspace.
- Longer keys are more secure but are also more resource intensive and can affect throughput.

DES Key Length	Keyspace	# of Possible Keys
56 bit	2^{5}	72,000,000,000,000,000
57 bit	2^{57}	144,000,000,000,000,000
58 bit	2^{58}	288,000,000,000,000,000
59 bit	2^{59}	576,000,000,000,000,000
60 bit	2^{60}	1,152,000,000,000,000,000

Types of Cryptographic Keys

- Symmetric keys that can be exchanged between two routers supporting a VPN.
- Asymmetric keys that used in secure HTTPS applications.
- Digital signatures that used when connecting to a secure website.
- Hash keys that used in symmetric and asymmetric key generation, digital signatures, and other types of applications

	Symmetric Key	Asymmetric Key	Digital Signature	Hash
Protection up to 3 years	80	1248	160	160
Protection up to 10 years	96	1776	192	192
Protection up to 20 years	112	2432	224	224
Protection up to 30 years	128	3248	256	256
Protection against quantum computers	256	15424	512	512

Choosing Cryptographic Keys

- Performance is another issue that can influence the choice of a key length.
- An administrator must find a good balance between the speed and protective strength of an algorithm.

Shorter keys equal faster processing, but are less secure.

Longer keys equal slower processing, but are more secure.

Questions?

End of Lecture 6