7.1.13 Cryptographic Attack Facts

Hackers attempt to figure out a way to get to data they want. Encrypting data is usually relatively secure, but there is unfortunately no such thing as a sure thing when it comes to protecting data. By using different types of attacks, hackers might be able to gain access to encrypted data.

This lesson covers the following topics:

- Common cryptographic attacks
- Future of cryptography

Common Cryptographic Attacks

The following table covers some of the more common cryptographic attacks.

Attack Method	Description
Dictionary	A dictionary attack is a type of brute-force attack. The hacker uses a list of words and phrases to try to guess the decryption key. ▪ Dictionary attacks work well if weak passwords are used. ▪ Using longer and uncommon passphrases is the best way to secure data against these attacks.
Collision attack	A collision attack tries to find two inputs that produce the same hash value. This type of attack is often used on digital signatures. ▪ If a hacker wanted to get User2 to sign a document by making it seem like it came from User1, the hacker would generate two documents that generate the same hash. ▪ The hacker would send one document to User1 and get that signature. ▪ The signature would be attached to the second document and sent to User2. Because the hashes are identical, User2 thinks the document is legitimate and has been signed by User1. Generating longer hash outputs is the key to stopping these types of attacks.
Birthday attack	This attack combines a collision attack and brute-force attack. The name is taken from the birthday probability math problem. The birthday probability math problem states that if you have 30 people in a room, the probability that someone has the same birthday as you is approximately 8%. However, the probability that any two people in the room have the same birthday is 70%. This is because we're not looking for an exact match (just any match), so the probability is higher. Digital signatures can be susceptible to birthday attacks. Generating longer hash outputs is the key to stopping these attacks.
Downgrade attack	A downgrade attack forces the system to use an older, less secure communication protocol. ▪ SSL exploitation is a common implementation of this attack. A hacker can set up their computer to only use SSL so that when the request is sent to the server, the server

downgrades from TLS to SSL to communicate. This then allows the hacker to launch SSL-based attacks on the server.
- Downgrade attacks are often used as part of a man-in-the-middle (MITM) attack. The hacker can intercept a HTTPS packet and downgrade it to a HTTP packet. If the server is not configured properly, the server responds using HTTP. This allows the hacker to now see all communications.

To prevent downgrade attacks, servers must be set up to not support these older and less secure protocols. Proper server configuration is the key to stopping these types of attacks.

Future of Cryptography

The future of computers and cryptography lies in quantum computing.

Classic computing works by processing bits of 1s and 0s. These bits represent electrical signals, on and off. Quantum computing uses qubits which can exist as both a 1 and 0 at the same time. Quantum computing is exponentially more powerful than today's computing standards.

This increased computing power means that today’s encryption standards can be hacked easily and quickly. An encryption key that might take years to crack with today’s computers can take days or even hours with quantum computers.

To combat the inevitable increase of quantum computing, researchers have already started work on post-quantum cryptography. These new methods will be used to ensure the safety of our data in the future.