UC Berkeley, MICS, W202-Cryptography

Week 08 Breakout 2

Modes of Operation

NIST SP 800-38A Defines 5 Modes of Operation

- ECB – Electronic Code Book
- CBC – Cipher Block Chaining
- CFB – Cipher Feedback
- OFB – Output Feedback
- CTR – Counter

Discussion Questions

1. In which of the 5 modes above would a bad ciphertext block damage the remaining decryption? In which modes would it only harm a few blocks? In which modes would it have no effect on remaining decryption?

2. In which of the 5 modes is the decryption algorithm needed? Not needed?

3. In which of the 5 modes can we precompute?

4. In which of the 5 modes can we precompute in parallel? (hint: only 1)

5. Do you agree or disagree with my personal opinion that all "salt" should be different for each encryption and should be encrypted using ECB with the key as the first block?

6. Of these 5 modes, Counter CTR Mode is most widely used. Discuss.

7. Back in the mid-1990's, a group of consumer electronics companies got together to design an encryption standard for DVD's. In addition to off the shelf videos, this was also used for software in which the general public could use to burn their own DVD's. They used a secret key that only industry insiders would have access to. They used an IV that was never changed. It was quickly broken. Discuss why. What are the inherent problem with encrypting video?

8. We have an operational database of 5 TiB of data. We perform a backup every day at the storage layer (on the filer) using snapshots so as not to impact our production database. A lot of data in the operational database is repeated. We know our backup files have 100% integrity verified by our filer. We want to both encrypt and compress our backups. We have a secure electronic key vault and catalog system which can generate and store unique keys, IV's, and nounces for each backup and associate them with backups in case we need to restore. Which should we do first, encrypt or compress? Suppose one day we need to restore from our backup and 1 byte in 1 block in the backup file is wrong, can we restore? (why DBAs and Cybersecurity Engineers frequently have conflict)

   Design an encryption / decryption solution for the above.

9. A traffic signal has a computer in the metal control box. It has several sensors mounted in various locations to measure the number of cars waiting in each direction and they wirelessly send information to the computer every 10 seconds. We must encrypt the data sent by the sensors. The data they send is really small, 4 bytes, so we don't want to wait until we get the full 16 bytes to decrypt and make use of the data. The traffic signal is set to run each direction for 30 seconds by default. If the event of heavy traffic limited to 1 or 2 directions, it can only make simple changes to the timing of individual directions to set them to 60 seconds, 90 seconds, or 120 seconds. It cannot make other changes to the traffic pattern for safety reasons. This feature of adjusting the timing for unbalanced traffic is a "nice to have" and not a matter of safety.

   Design an encryption / decryption solution for the above.

10. A railroad has installed numerous sensors on the tracks to help guard against derailments and "cornfield meets" (head to head on the same track), and to monitor that trains are being operated within laws and safety regulations. Sensors send data via the cell phone network from remote areas. They send data at various increments, from 10 seconds to 1 minute depending on the sensor, but sensors can be bursty. The sensor data is often much smaller than 16 bytes. There is a central computer which can warn of impending danger and if necessary send an emergency stop signal to any train. We want to process data as soon as possible. An emergency stop signal is extremely dangerous and we only want to send it as a last resort, so any bad data can be a matter of life or death. Also, trains are considered a high value target for terrorists.

    Design an encryption / decryption solution for the above.

11. We are flying drones remotely from around the world. Just concentrate on the video. Suppose we receive video at 30 frames per second from satellites (one way – use it or loose it). We need to encrypt it. It can be very noisy at times.

Design an encryption / decryption solution for the above.

12. Time permitting, for each of the 5 modes, discuss scenarios that would be especially good fits for each mode.