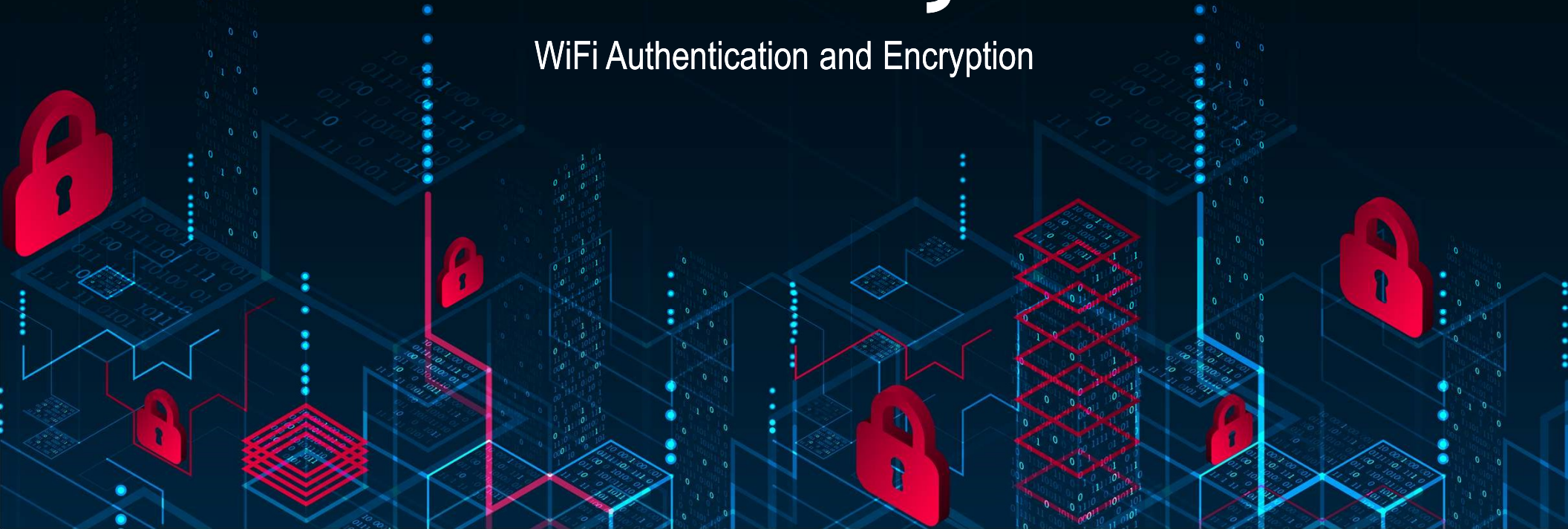


CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Wireless, IoT, and Cloud Security

WiFi Authentication and Encryption



Video summary

- WiFi Authentication Modes
- WiFi Encryption
- WEP, WPA, and WPA2
- Procedures to Improve Wireless Security

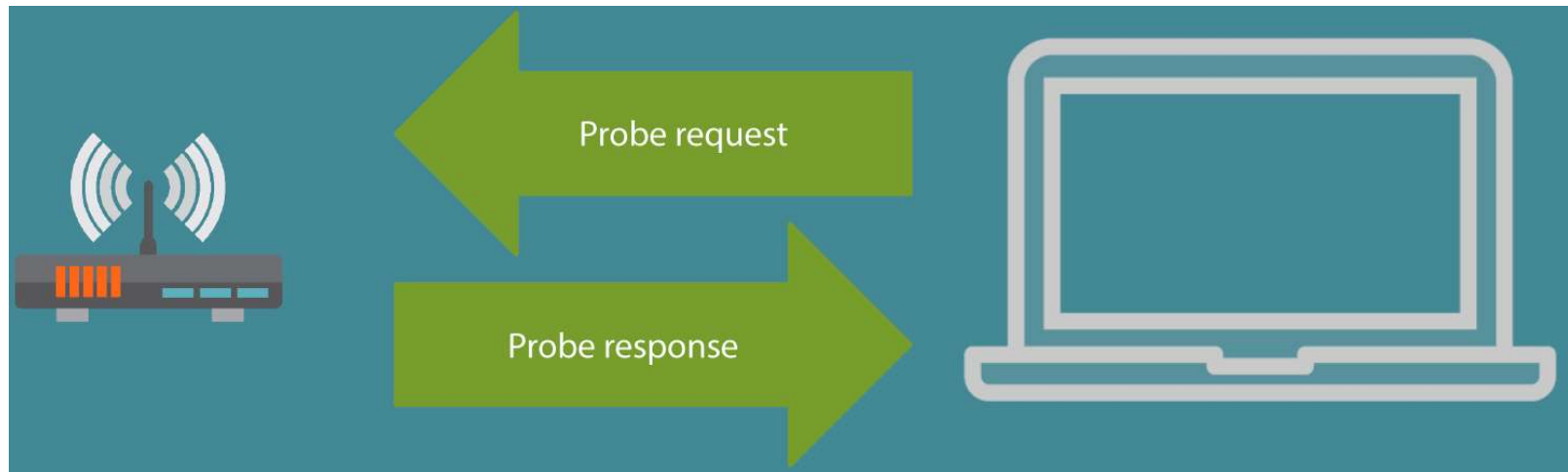


WiFi Authentication

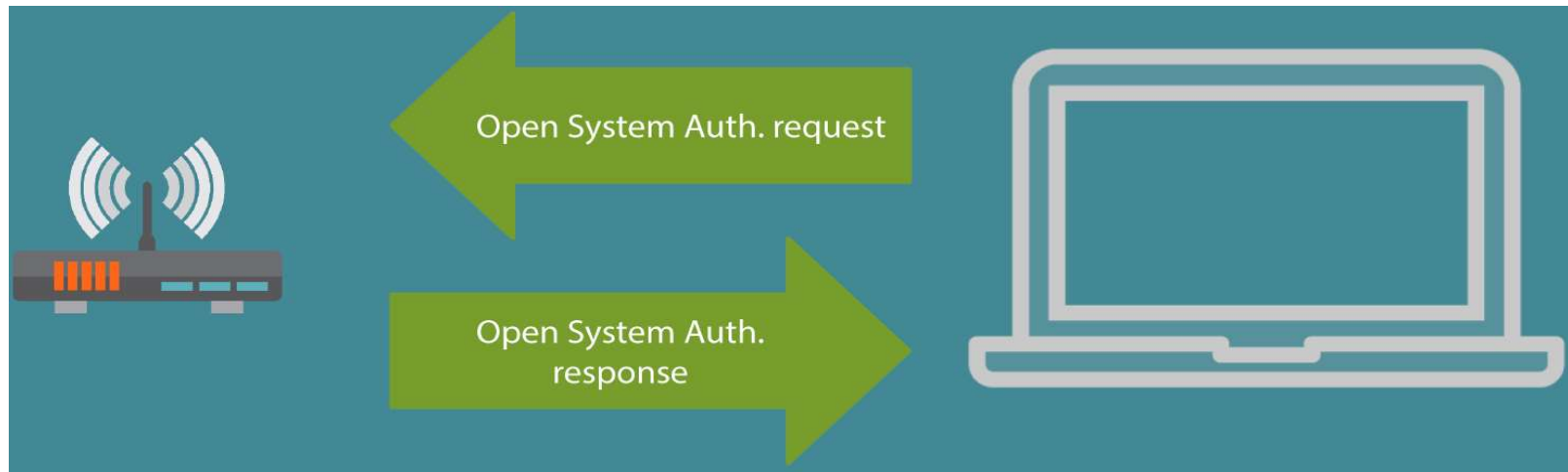
- Open System Authentication
- Shared Key Authentication
- IEEE 802.1X



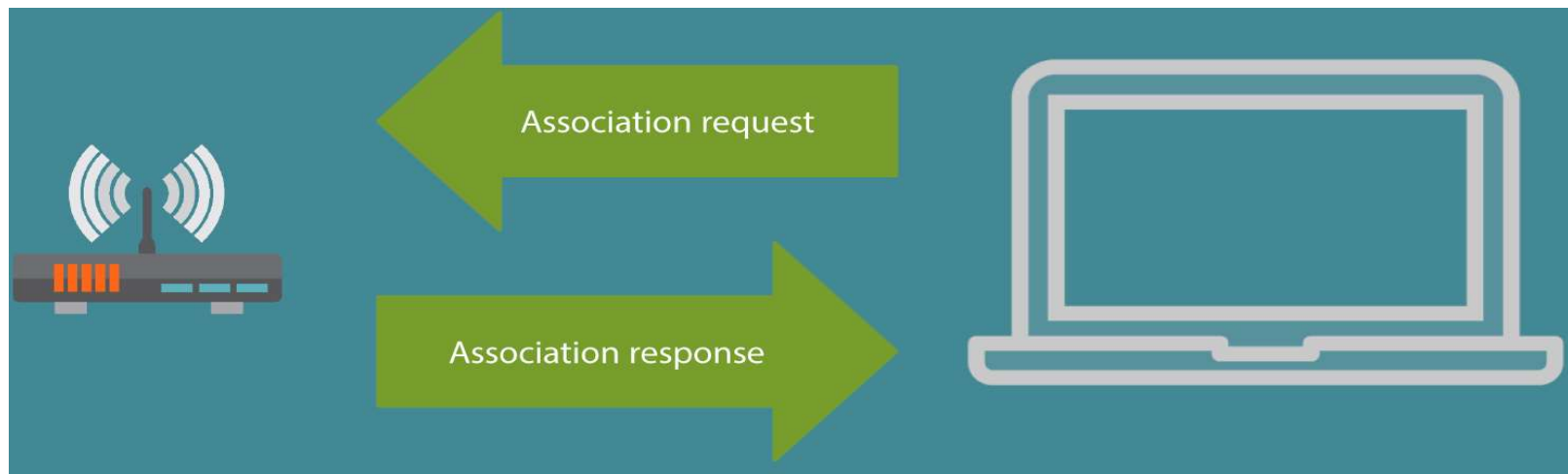
Open System Authentication



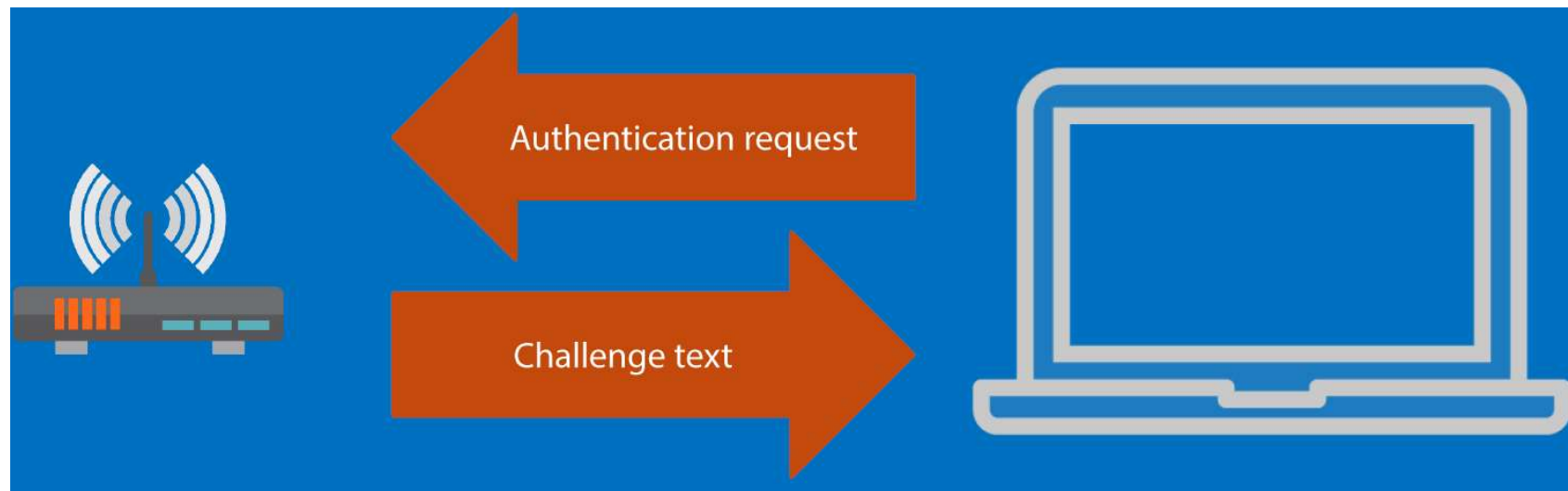
Open System Authentication



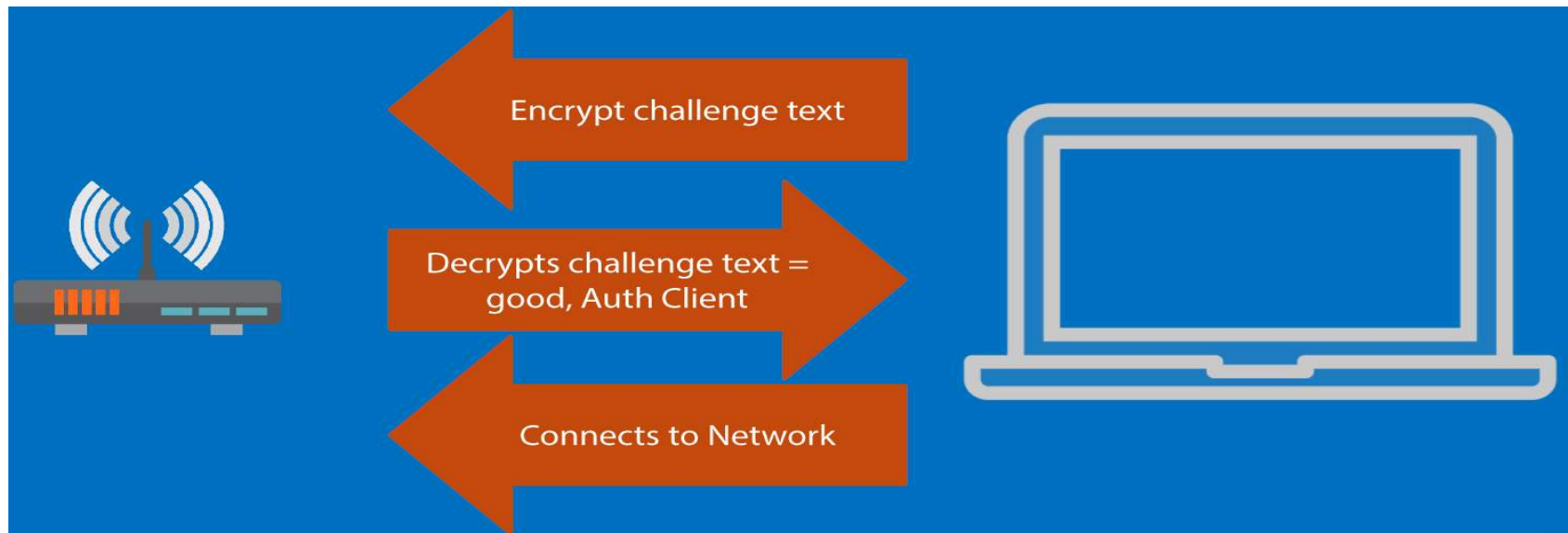
Open System Authentication



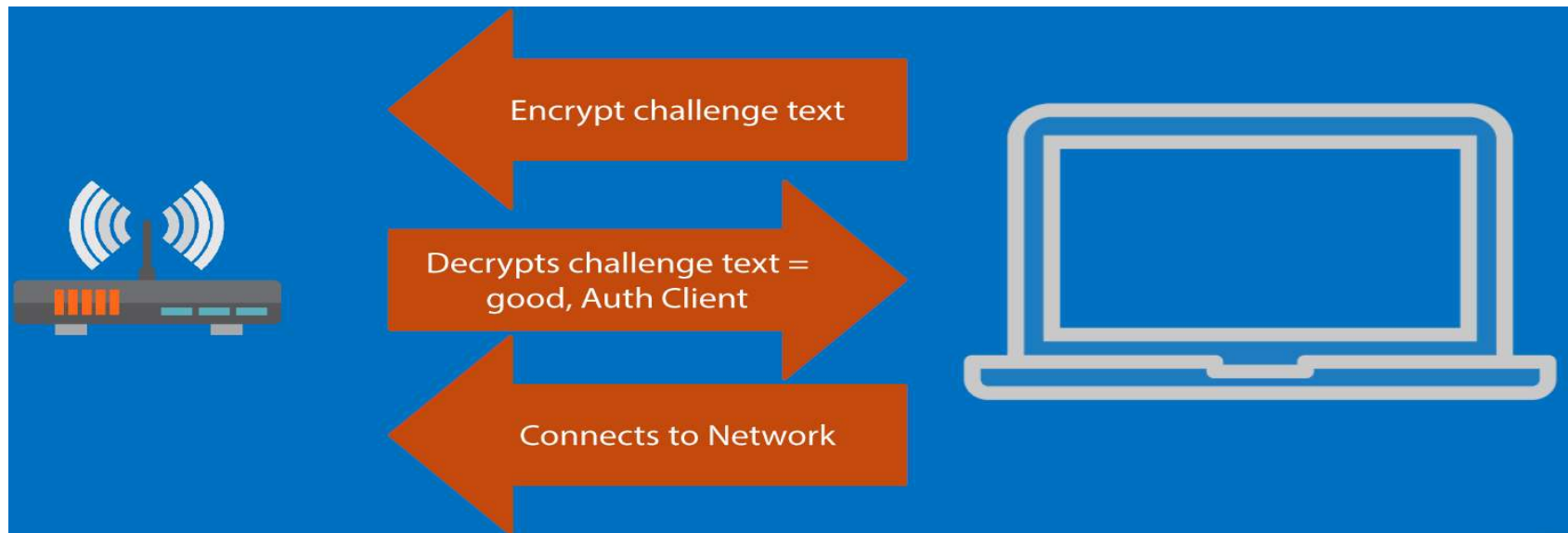
Shared Key Authentication



Shared Key Authentication



Shared Key Authentication



WiFi Encryption

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)



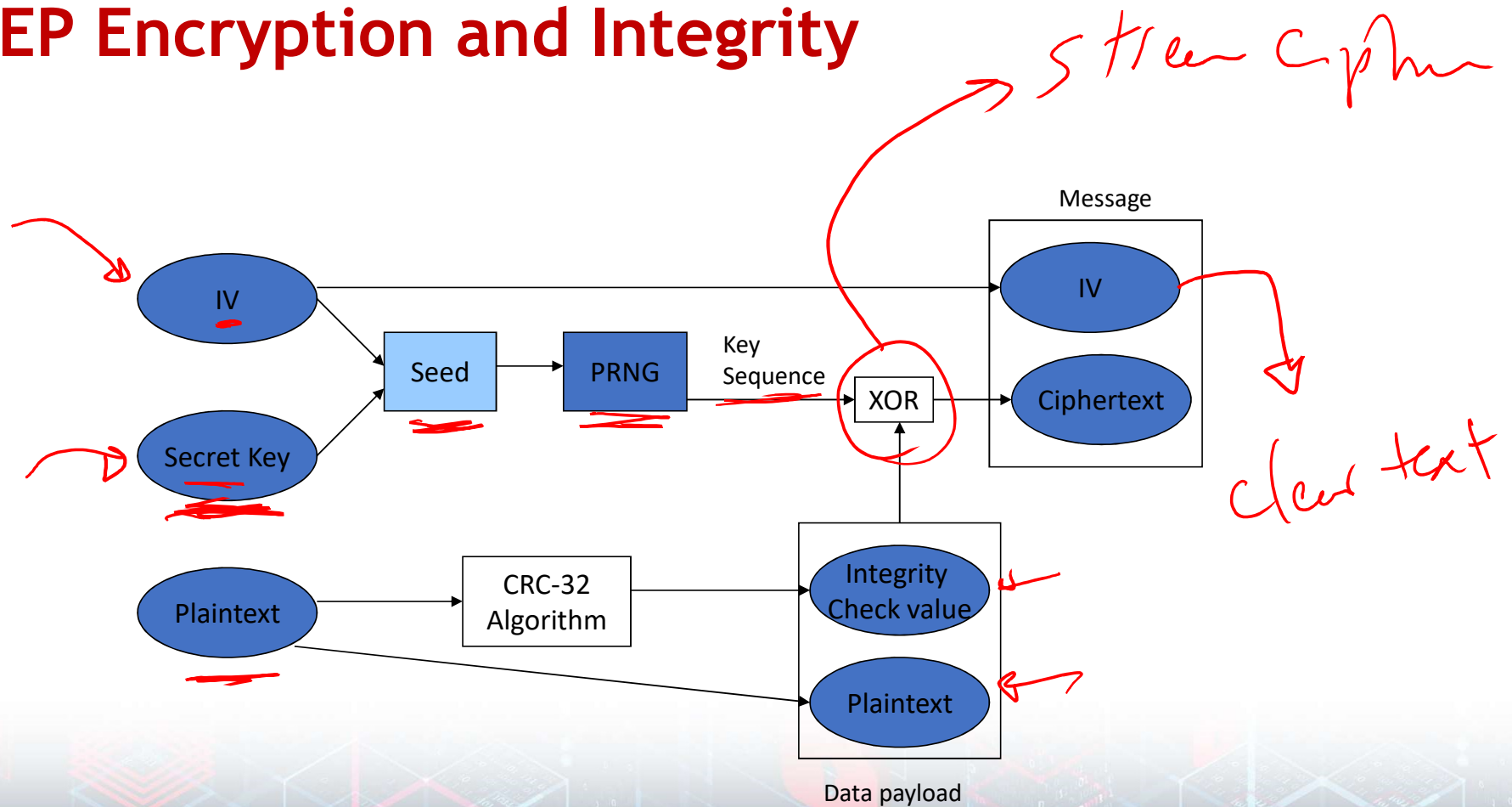
Wired Equivalency Protocol (WEP)

- The original native security mechanism for WLAN
 - Uses an RC4 stream cipher.
 - Pseudo-random bytes.
 - Two versions: 64-bit and 128-bit versions.
- Used to protect wireless communication from eavesdropping (confidentiality)
- Prevent unauthorized access to a wireless network (access control)
- Uses static encryption keys.
 - Easy to crack (short IV and static key)

Block
stream



WEP Encryption and Integrity



PRNG – RC4 Pseudorandom number generation algorithm

WEP Flaws and Vulnerabilities

- Weak keys:
 - ✓ It allows an attacker to discover the default key being used by the Access Point and client stations
 - ✓ This enables an attacker to decrypt all messages being sent over the encrypted channel.
- IV (initialization vector) reuse and small size: 24-bit
 - ✓ There are 2^{24} different IVs
 - ✓ On a busy network, the IV will surely be reused, if the default key has not been changed and the original message can be retrieved relatively easily.

Attacks on WEP

- WEP encrypted networks can be cracked in seconds
- Goal is to collect enough IVs to be able to crack the key



```
Shell - Konsole <3>
Session Edit View Bookmarks Settings Help

* Got 5060091 unique IVs | fudge
* Elapsed time [00:00:05] | tr

KB depth votes
0 0/ 1 D0(1204) 58( 55) F8( 40) 80( 3C( 30) 04( 30) 94( 25) C7( 23) C4( 20)
1 0/ 1 05( 748) 93( 58) E3( 33) 18( 21) 6E( 20) 19( 15) 31( 15) A1( 15) E6( 15)
2 0/ 1 E9( 100) 08( 12) 0E( 8) 0F( 8) DC( 3) 27( 0) 60( 0) 89( 0) 97( 0)
3 0/ 1 EA( 164) 7E( 9) 19( 5) 38( 3) 9A( 3) FF( 3) 1F( 0) 20( 0) A8( 0)
4 0/ 1 34(1780) 21( 27) 0D( 18) 47( 12) B7( 8) FC( 6) 2E( 3) 2F( 3) 8D( 3)
5 0/ 1 51( 151) C0( 13) 08( 10) 60( 8) C7( 8) 7B( 3) D0( 3) D1( 3) D2( 0)
6 0/ 1 94( 84) 75( 38) 92( 38) 21( 22) 80( 19) 6C( 15) 7E( 15) 77( 13) 5C( 12)
7 0/ 1 13( 214) CE( 23) 51( 20) D6( 20) F8( 19) FA( 19) 08( 15) 83( 6) 94( 6)
8 0/ 1 E0(1017) C2( 36) C0( 27) AA( 25) 9F( 19) B1( 18) 0A( 18) D8( 16) AE( 15)
9 0/ 1 68( 200) D6( 30) B1( 16) 79( 15) B2( 15) E3( 15) C0( 11) C2( 8) C3( 8)
10 0/ 1 D3( 728) D7( 93) 71( 88) 3C( 65) 54( 63) 78( 54) 6F( 53) 69( 51) 5C( 50)
11 0/ 1 20( 236) 31( 23) 7B( 22) 8A( 20) EA( 20) 88( 19)
12 0/ 1 42( 126) 5E( 45) BA( 23) 3A( 21) 65( 21) 66( 19)

KEY FOUND! [ 0005E9EA34519413E068032042 ]

root@1[wepcrack]#
```


Wi-Fi Protected Access (WPA)

stream cipher

❖ This is a new standard from the Wi-Fi Alliance that uses the 40 or 104-bit WEP key, but it changes the key on each packet.

- Firmware update to replace WEP. ✓
- 128-bit Temporal Key Integrity Protocol (TKIP) encryption.
 - Uses a master key that is regularly changed.
- Improved data encryption (48 bit IV)
- Strong user authentication



WEP vs. WPA

	WEP	WPA
Encryption	Flawed	Fixes all WEP flaws
	40-bit keys	128-bit keys
	Static-same keys used by everyone on network	Dynamic session keys. Per-user, per-session, per-packet keys
	Manual distribution	Automatic Distribution
Authentication	Flawed, uses WEP key itself	Strong user authentication using 802.1X and EAP

Wi-Fi Protected Access 2 (WPA2)

Block

- Designed to replace WEP.
 - 128-bit Advanced Encryption Standard (AES).
- The primary enhancement over WPA is the use of the AES (Advanced Encryption Standard) algorithm
- Based on the IEEE 802.11i standard.
- Uses PSK (256 bit key) and 8-63 ASCII Characters

WPA2

- WPA2 has immunity against many types of hacker attacks
 - ✓ Man-in-the middle
 - ✓ Authentication forging
 - ✓ Replay
 - ✓ Key collision
 - ✓ Weak keys
 - ✓ Packet forging
 - ✓ Dictionary attacks



WEP vs WPA vs WPA2

	WEP	WPA	WPA2 ✓
→ ENCRIPTION	RC4	RC4	AES
→ KEY ROTATION	NONE	Dynamic Session Keys	Dynamic Session Keys
→ KEY DISTRIBUTION	Manually typed into each device	Automatic distribution available	Automatic distribution available
→ AUTHENTICATION	Uses WEP key as Authentication	Can use 802.1x & EAP	Can use 802.1x & EAP

Procedures to Improve Wireless Security

- Use wireless intrusion prevention system (WIPS)
- Use WPA2 where possible
- Use a good + long passphrase
- AES is more secure, use TKIP for better performance
- Change your SSID every so often
- Wireless network users should use or upgrade their network to the latest security standard released

IDS

Block/Stop



Video summary

- WiFi Authentication Modes
- WiFi Encryption
- WEP, WPA, and WPA2
- Procedures to Improve Wireless Security

