1. Wat is het verschil tussen b’hello world` en “hello world”?

Zonder b is het een string. Met de b erbij is het een byte string.

1. Kun je encryptie vervangen met encodering? Waarom zou dit wel of niet een probleem zijn?

Nee, ze hebben verschillende doelen.

* Encodering zet gegevens van het ene formaat om naar het andere formaat.
* Encryptie zet gegevens om in onleesbare taal. Meestal doormiddel van een sluitel.

1. wat is er uniek aan de uitkomst van CX XOR K, en waarom zou dit nuttig zijn voor cryptografie?

XOR is omkeerbaar. Als je de operatie nogmaals uitvoert met dezelfde bit patronen, je terugkeerd naar het oorspronkelijke bericht. Dit is handig voor symmetrische cryptografie, omdat je dezelfde sleutel gebruikt voor het coderen en decoderen.

Op basis van de sleutel kun je bepalen of de ciphertekst is versleuteld met AES-128, AES192, of AES-256. Welke is het, en hoe weet je dat?

De sleutel SECRETSAREHIDDEN bestaat uit 16 karakters. 1 ascii karakter heeft 7 bits met 1 significant bit. Dus bestaat uit 8 bits. Dat is precies 1 byte. Daarom de som 16\*8=128.

1. Leg in je eigen woorden duidelijk uit deze extra stap in CBC de bovengenoemde kwetsbaarheid in ECB-mode oplost.

Omdat hij de XOR operatie uitvoert op het vorige blok. Zo komt er elke keer weer een unieke cipherblok terug.

1. . Leg uit hoe je door de vorige opdracht kon zien wat de blocksize is. Met welke eigenschap van ECB mode heeft dit te maken?

Hexidecimaal terug rekenen naar binar. De random key generator is 16. Dat is dezelfde lengte als de key van de vorige opdracht.