Computer Security (COM-301)

Applied cryptography I

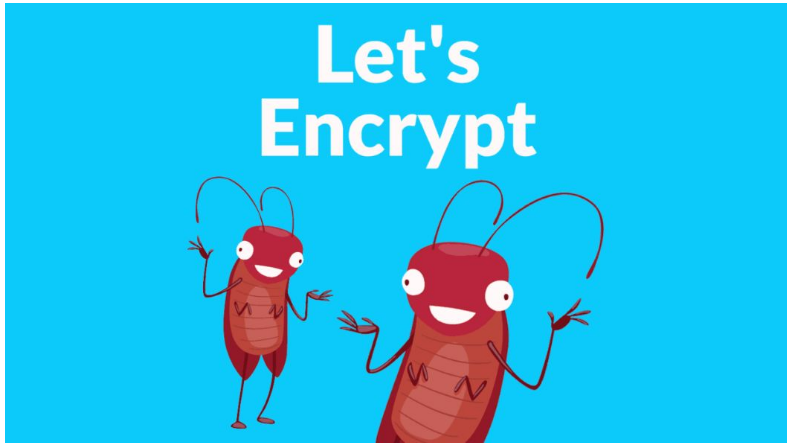
Interactive Exercises

Carmela Troncoso

SPRING Lab

carmela.troncoso@epfl.ch

OTP is the best?



Agree or disagree and justify :

“A One Time Pad is the best choice to transmit a secret document of 10Mb because we know it provides perfect secrecy”

Secure streaming

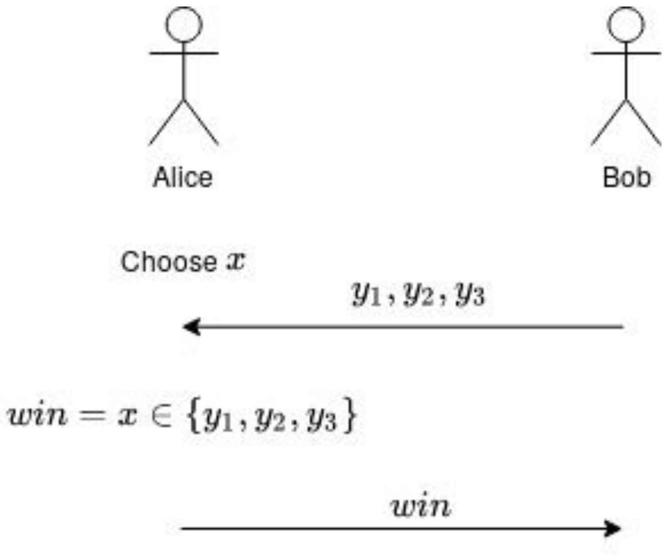
Is the following pseudocode for a function to encrypt movies a secure use of a stream cipher? Justify your answer.

```
var iv = "bestidever“

def EncryptMovie(movie):
   key = GenerateSecureRandomKey() // generates a truly random key
   secureKeyTransfer(key)  // securely sends the key to the
               // recipient
   EncryptedMovie = Salsa20(key,iv,movie) // uses Salsa20 stream
                        // cipher
   return(EncryptedMovie)
```

Guess my number

Alice and Bob have decided to play a game called "Guess my number". In this game, Alice chooses one number between 0 and 100. Then, Bob has 3 chances to guess the number. Bob wins if he guesses the number correctly. How can Alice cheat? Bob thinks that using a Message Authentication Code (MAC) can prevent cheating. Can you integrate MAC into this game in a way that allows Bob to publicly show that Alice has cheated? What if Alice and Bob have a trusted friend called Charlie and Bob only cares about Charlie's opinion? Justify your answers.



Encrypt full speed

You are designing a high-speed encrypted link between two buildings at your company. What symmetric encryption scheme would you use if

- There is only one core in the receiver and transmitter

- There are several cores in the receiver and the transmitter

OTP or AES

Alice knows that she will want to send a single 128-bit message to Bob at some point in the future. To prepare, Alice and Bob first select a 128-bit key $k \in \{0, 1\}$ 128 uniformly at random.

When the time comes to send a message $x \in \{0, 1\}$ 128 to Bob, Alice considers two ways of doing so:

1) She can use the key as a one time pad, sending Bob $k \oplus x$.

2) She can use AES to encrypt x. Recall that AES is a 128-bit block cipher which can use a 128-bit key, so in this case she would encrypt x as a single block and send Bob $AES_k(x)$.

Assume the adversary Eve will see either $k \oplus x$ or $AES_k(x)$, that Eve knows an initial portion of x (a standard header), and that she wishes to recover the remaining portion of x. If Eve is an all powerful adversary and has time to try out every possible key $k \in \{0, 1\}$ 128, which scheme would be more secure?