IT Security ECB vs CCB

Michael Claudius, Associate Professor, Roskilde

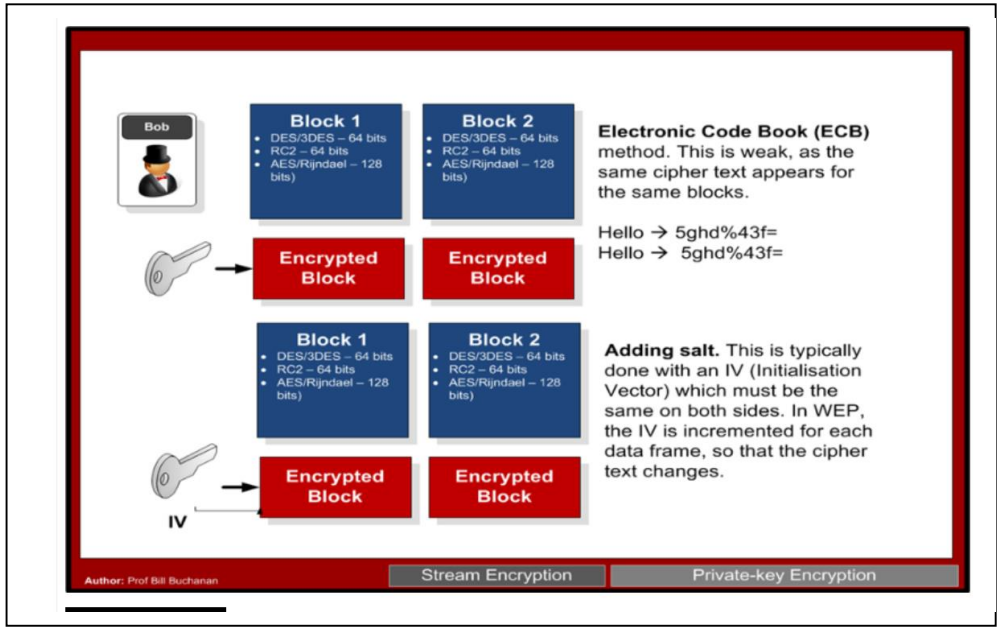
20.08.2024

Problems with Block Ciphers

- **Same Plain text (P) results in same Cipher text (C)**
- **Solution Salting**
  - **Random number for each block**
  - **Initialization Vector (IV)**
- **Parallel computing not possible ?**
-
- **Lets look a little deeper into the problem and solutions**

Electronic Code Book (ECB)

- **Typical block sizes are 64, 128 or 256 bytes.**
- **Unfortunately, the cipher blocks could end up being the same, for the same input text.**
- **Thus an intruder could try and guess the cipher text. This is known as electronic code book (ECB).**
- **Use 3DES to encrypt the word “fred”, with a key of “bert12345”, we will always get: HgvGuzedMg8=**



ECB (Electronic Code Book) Text Example

In ECB (Electronic Code Book) we have repeating cipher blocks for the same plain text.

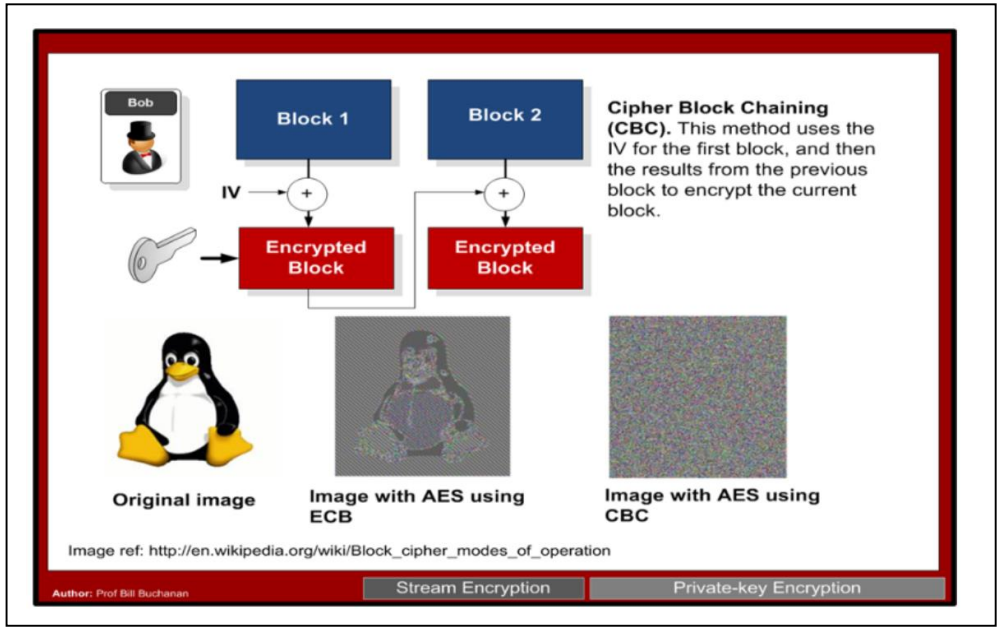
- **If I take "eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee" and encrypt with 3-DES and a key of "bill12345" we get:**
  1122900B30BF1183 1122900B30BF1183 1122900B30BF1183 1122900B30BF1183 1122900B30BF1183 1122900B30BF1183 7591F6A1D8B4FC8A

- **The "e..e" values are always coded with the same cipher text. As 3-DES has message blocks of 64-bits, then 8 'e' values will fill each block.**
- **[eeeeeeee] [eeeeeeee] [eeeeeeee] [eeeeeeee] [eeeeeeee] [eeeeeeee] [eeeeee padding]**

- **Thus we can say that "eeeeeeee" maps to the cipher text of 1122900B30BF1183**

CBC (Cipher Block Chaining) Image Example

- **The method most often used is CBC (Cipher Block Chaining), where we start off with a random seed, known as an Initialization Vector (IV). This is then used to create the first block.**
- **Next the output from the first block is then used to chain into the next block by Exclusive-OR'ing the output of the first with the output of the second block, and so it goes on.**



- **All good ? Do you see any defects of CBC ?**

Counter (CTR) vs CBC

- **Problem: One issue with CBC is the encryption and decrption processes will be slow, as each stage depends on the previous stage, and we thus cannot apply parallel processing**.

Solution:

- **Counter (CTR) mode.**
- **Counter (CTR) mode converts the block cipher into a stream cipher. With this it generates a counter value and a nonce, and encrypts this, in order to EX-OR with the plain text block.**
- **The counter can increment by one each time, or can use a given algorithm (known only be the sender and trusted receiver). The advantage of this method is that the processing of each block is independent of the others, so we can apply parallel processing to each.**

- **BUT it is not safe as CBC!**

Exercise

- **It is time for discussion, applying encryption algorithms**
- **Also we will investigate the Homework 1 exercise !!**

- Lab Cryptool 1
- Homework1: Security Attacks

- ***Look at details, but don't loose the overview ☺***
- ***Just follow the "right" track and you find the gold***