Tutorial 3

**School of Digital Media and Infocomm Technology ST2504 Applied Cryptography**

1. a) Describe the TWO differences between the Rijndael and AES encryption algorithms.

**AES has a fixed block size of 128-bits, and key-sizes of 128, 192 and 256-bits. This is in accordance with the requirements of the AES development procedure.**

**Rijndael allows for the block and key sizes to be any multiple of 32-bits between 128 and 256 inclusive.**

* 1. Explain why AES is an “iterative” cipher.

**Because AES processes data as block of 4 columns of 4 bytes and operates on entire data block for multiple times (depending on the key size).**

* 1. State 3 design characteristics of AES cipher.

**Resistant against known attacks.**

**Speed and code compactness on many CPUs.**

**Design simplicity.**

1. a) State the 4-step encryption process of the AES cipher.

**Step 1: Byte substitution (S-box used on every byte)**

**Step 2: Shift rows (permute bytes between groups/columns)**

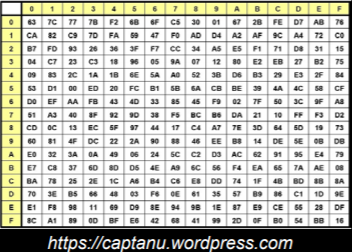
**Step 3: Mix columns (subs using matrix multiplication of groups)**

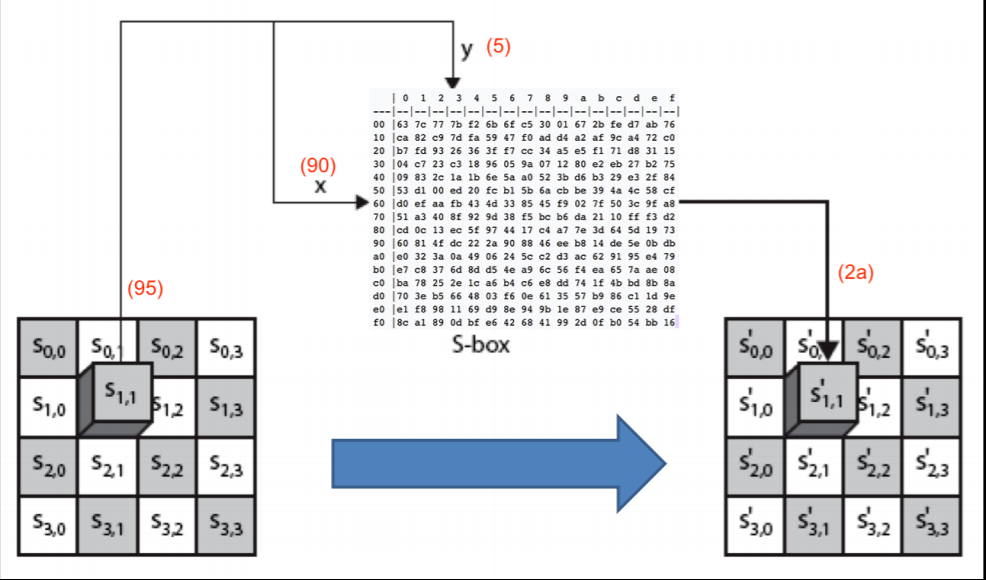
**Step 4: Add round key (XOR state with key material)**

***\*refer to lecture notes slides 9-17 for all 4 steps of the encryption process***

* 1. With the aid of a diagram, illustrate and describe the first 2 steps encryption process of the AES cipher.

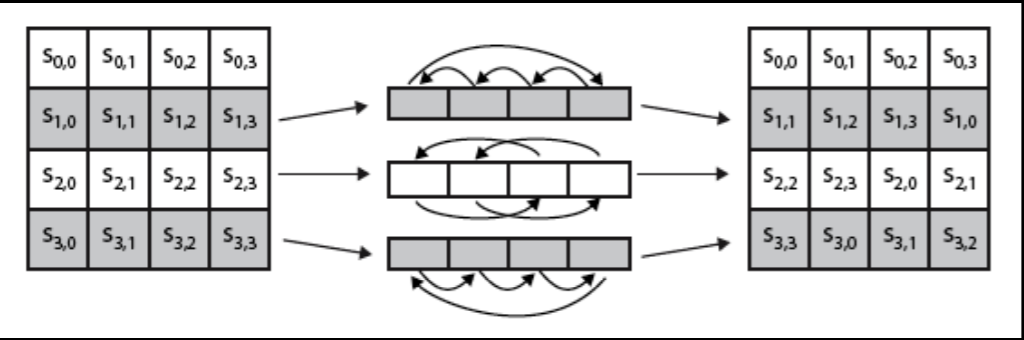
**Step 1: “Byte substitution” step in AES**





* **In this “Byte substitution” step, the S-box technique is used**
* **Uses data block of 4 columns of 4 bytes**
* **Uses one table of 16x16 bytes containing a permutation of all 256 8-bit values**
* **The input plain text passes the S-box and the corresponding text is generated**
* **Note that one S-box is used for one complete cipher**

**Step 2: “Shift rows” step in AES:**



* **A circular byte shift in each row**
* **1st row is unchanged**
* **2nd row does 1 byte circular shift to left**
* **3rd row does 2 byte circular shift to left**
* **4th row does 3 byte circular shift to left**
* **Decrypt inverts using shifts to right**
* **This step permutes bytes between the columns**

ACG/ST2504 1 May 2018