**DATA SECURITY**

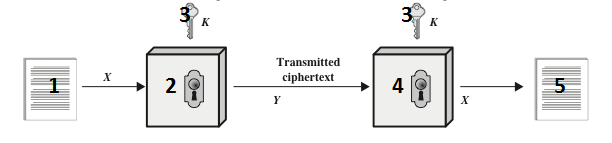
**1.** Substitution is an operation in which each element in the plaintext (bit, letter, group of bits, or letters) is mapped into another element. **True**

**2.** The AES cipher consists of N rounds, where the number of rounds depends on the **key length**

**3.** Caesars cipher involves replacing each letter of the alphabet with the letter standing k places further down the alphabet **True**

**4.** Explain the Symmetric encryption scheme (explain ingredients).

Please write proper annotations :



**1. Plaintext input - unencrypted data that the sender wants to protect**

**2. Encryption algorithm(e.g. AES) - mathematical process used to transform the plaintext into ciphertext**

**3. Secret key shared by sender and recipient**

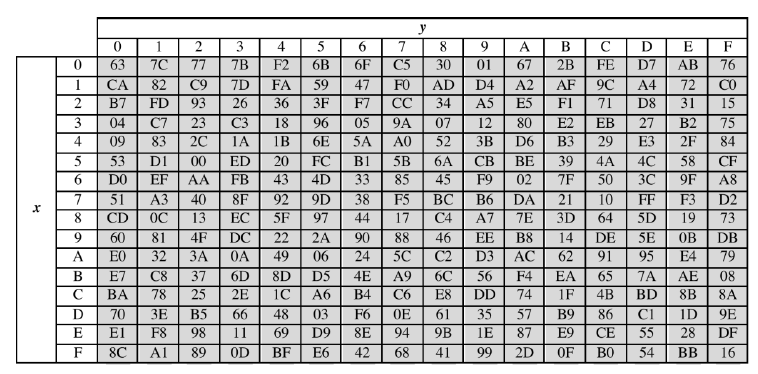
**4. Decryption algoritm (reverse of encryption algorithm) - mathematical process used to reverse the encryption and retrieve the original plaintext from the ciphertex**

**5. Plaintext output**

**Encryption Y = E(K, Y) - Y is the ciphertext, K is the secret key used for encryption, E is the encryption algorithm**

**Encryption X = D(K, Y) - X is the original plaintext, K is the secret key used for decryption, D is the decryption algorithm**

**5.** According to the S-Box below, to which hexadecimal value would the byte value 0000 0001 be substituted? Please note that 1 byte (8 bits) of information can be represented with 2 hexadecimal digits (1 hexadecimal digit for a block of 4 bits)



**0000 = 0 in hexadecimal (x-side)**

**0001 = 1 in hexadecimal (y-side)**

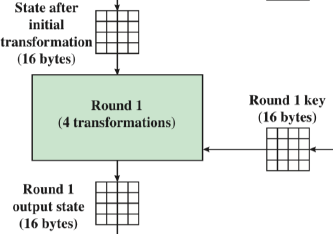
**result = 7C (the cross point)**

**Different example: 101111**

**We take the first and the last digit in binary and convert them in hexadecimal => 11 = 3 in hexadecimal;**

**We take the middle digits and convert them in hexadecimal => 0111 = 7 in hexadecimal**

**6.** Please name the four transformations taking place in each round of the AES protocol (see the depiction below)



**Four different stages/transformation functions are used in each round, one of permutation and three of substitution**

**1. SubBytes – uses an S-box to perform a byte- by-byte substitution of the block**

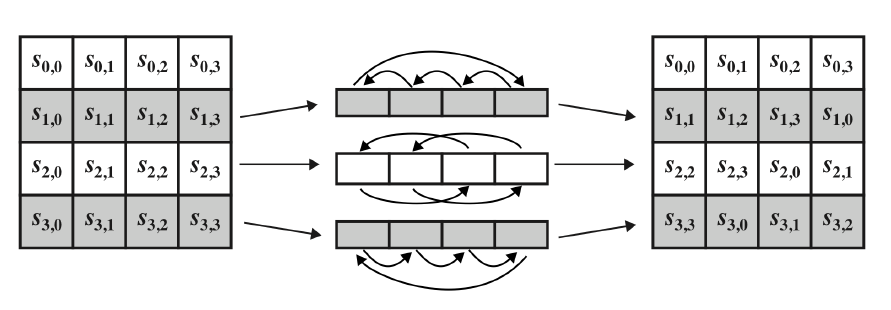
**2. ShiftRows – a simple permutation**

**3. MixColumns – a substitution that makes use of arithmetic over GF(28)**

**4. AddRoundKey – a simple bitwise XOR of the current block with a portion of the expanded key**

**7.** Please write down how the following 4 x 4 matrix will be transformed after performing a shift-row transformation in the AES protocol (as depicted below)

row 1: A1B1 A2B2 A3B3 A4B4 ------------>   
 row 2: B1C1 B2C2 B3C3 B4C4 ------------>  
 row 3: C1D1 C2D2 C3D3 C4B4 ------------>

row 4: D1A1 D2A2 D3A3 D4A4 ------------>   
  


**A1B1 A2B2 A3B3 A4B4 - Row 1 is not shifted**

**1C1B 2C2 3C3B 4C4B - Row 2 is shifted one position to the left**

**C3D3 C4B4 C1D1 C2D2 - Row 3 is shifted two positions to the left**

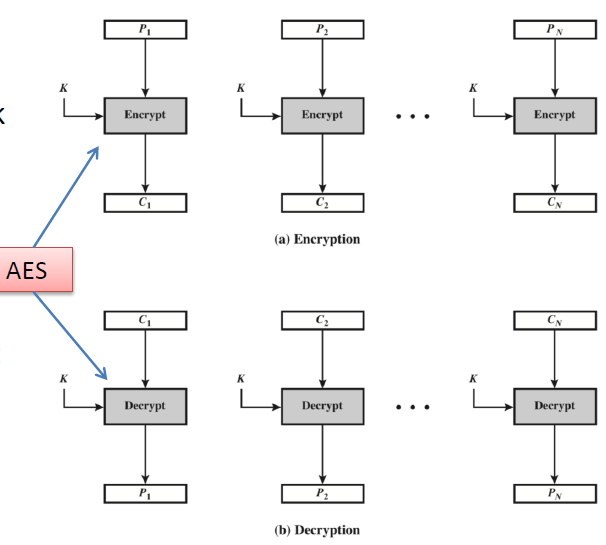
**D4A4 D1A1 D2A2 D3A3 - Row 4 is shifted three positions to the left**

**8.** How many rounds does AES cipher have? **10/12/14**

**9.** An advantage of the ECB mode of operation is that there is no error propagation **True**

**10.** In the ECB mode, the same plaintext block always produces the same ciphertext **True**

**11.** Please explain the main aspects and properties of the Cipher Block Chaining (CBC) mode from below



**• Same plaintext blocks produce different ciphertext blocks**

**• Same key K is used for each block**

**• Padding the last block if necessary**

**• After decryption algorithm (Decrypt), the result is XORed with the preceding ciphertext block to produce the plaintext block**

**• An initialization vector (IV) is XORed with**

**- First block of plaintext**

**- Output of the decryption algorithm of the first block**

**- Has same size as the cipher block**

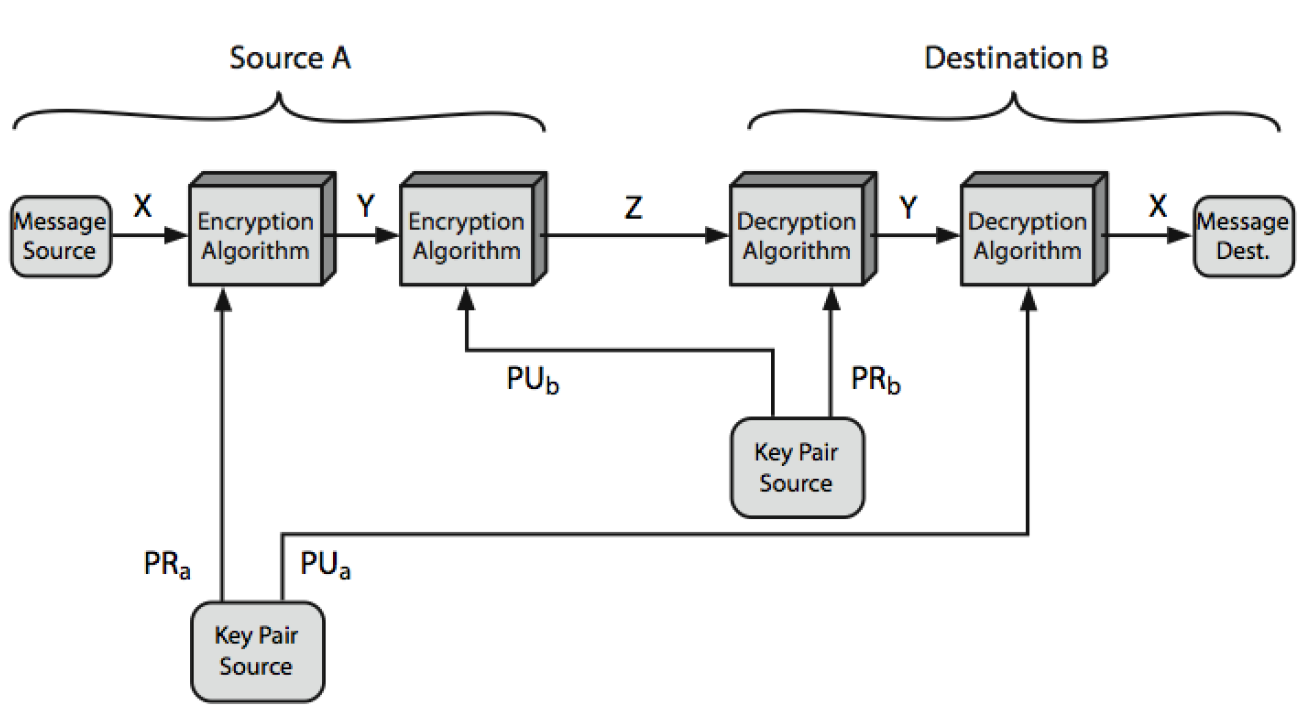
**- Must be known to both sides**

**12**. In the Cipher Block chaining Mode (CBC):

- same plaintext blocks produce different ciphertext blocks and different key K is used for each block **True**

**13**. In the Output Feedback (OFB) Mode (see below)  
- Bit errors in transmission do not propagate **True**

**14**. A disadvantage of the CTR mode is that encryption is done in parallel on multiple blocks **True**

**15.** Describe the details of the Public-Key Cryptosystem illustrated in the Figure. Does the cryptosystem provide authentication? What about secrecy? Explain   


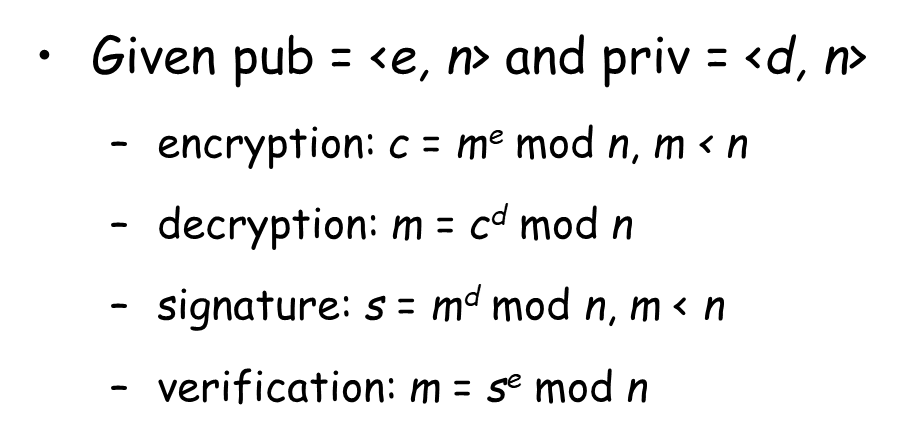
**We begin by encrypting a message, using the sender’s private key. This provides the digital signature. Next, we encrypt again, using the receiver’s public key**

**• The ciphertext can be decrypted only by the intended receiver, who alone has the matching private key. Thus, confidentiality is provided**

**• Then the receiver can verify the signature by using sender’s public key**

**• Authentication: Achieved through the digital signature, which can be verified using the sender's public key.**

**• Secrecy: Achieved through encrypting the message with the recipient's public key, ensuring only the recipient can decrypt it using their private key.**

16. Please explain through an example how RSA works. Why does RSA work? The modules of RSA are summarized below

**Encryption:  
 - Take a message and turn it into a number smaller than n.**

**- Raise this number to the power of e, and take the remainder when divided by n. This result is the encrypted message c**

**Decryption:  
 - The recipient uses the private key**

**- Take the encrypted message c, raise it to the power of d, and take the remainder when divided by n. This result is the original message m.**

**Signature:**

**- Raise m to the power of d, take the remainder, and get a signature s.**

**Verification:**

**- The recipient has the public key**

**- Raise the signature s to the power of e, take the remainder, and check if it matches the original message m.**

**- If they match, the signature is valid.**

**Why RSA Works?**

**- It's hard to figure out the private key from the public key because of the difficulty in factoring large numbers.**

**- The security is based on the fact that certain math problems are easy to do in one direction but very hard in the reverse direction.**

**In essence, RSA allows secure communication and signature verification by cleverly using big numbers and their properties. The security comes from the difficulty of solving specific math problems, making it challenging for anyone to break the system.**