Jamia Millia Islamia

Dept. Of Computer Science

Cryptography Assignment-2

Submitted By:Wasit Shafi

Roll no: 18MCA054

Submitted To:Dr.Rafat Parveen

Question 1: What was the original and final set of criteria used by NIST to evaluate candidate AES ciphers?

Solution:

The original set of criteria used by NIST to evaluate candidate AES cipher was:

- Security: Actual security; randomness; soundness, other security factors.
- Cost: Licensing requirements; computational efficiency; memory requirements.
- Algorithm and Implementation Characteristics: Flexibility; hardware and software suitability; simplicity.

The final set of criteria used by NIST to evaluate candidate AES ciphers was:

- General Security
- Software Implementations
- Restricted-Space Environments
- Hardware Implementations
- Attacks On Implementations
- Encryption vs. Decryption
- Key Agility
- Other Versatility And Flexibility
- Potential for Instruction-Level Parallelism

Question 2: List the parameters (block size, key size, and the number of rounds) for the three AES versions.

Solution:

AES Parameters(128 bit , 192 bit , 256 bit)

Key size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext block size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size (words/bytes)	44/176	52/208	60/240

Question 3: How many transformations are there in each version of AES? How many round keys are needed for each version?

Solution:

1. **Substitute Bytes Transformation**

Forward and Inverse Transformations

The forward substitute byte transformation, called SubBytes. AES defines a 16 x 16 matrix of byte values, called an S-box that contains a permutation of all possible 256 8-bit values.

Each individual byte of State is mapped into a new byte in the following way: The leftmost 4 bits of the byte are used as a row value and the rightmost 4 bits are used as a column value.

2. **ShiftRows Transformation**

Forward and Inverse Transformations

The forward shift row transformation, called Shift Rows. The first row of State is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2- byte circular left shift is performed. For the fourth row, a 3-byte circular left shift is performed.

3. **MixColumns Transformation**

Forward and Inverse Transformations

The forward mix column transformation, called MixColumns, operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column.

4. **AddRoundKey Transformation**

Forward and Inverse Transformations

In the forward add round key transformation, called AddRoundKey, the 128 bits of State are bitwise XORed with the 128 bits of the round key.

The operation is viewed as a columnwise operation between the 4 bytes of a State column and one word of the round key; it can also be viewed as a byte-level operation

Question 4: Compare DES and AES. Which one is bit-oriented? Which one is byte oriented?

Solution:

AES	DES
AES stands for Advanced Encryption Standard.	DES stands for Data Encryption Standard.
Key length varies from 128 bits, 192 bits to 256 bits.	Key length is of 56 bits.
Number of rounds depends on key length : 10(128-bits), 12(192-bits) or 14(256-bits)	16 rounds of identical operations
AES structure is based on substitution-permutation network.	DES structure is based on feistal network.
AES can encrypt 128 bits of plain text. hence, more secure.	DES can encrypt 64 bits of plain text. hence, less secure.
AES derives from Square cipher	DES derives from Lucifer cipher.
AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.

Note : whereas DES is a bit-oriented cipher, AES is a byte-oriented cipher.

DES requires bit-level access to the block coming into a round. On the other hand, all operations in AES are purely byte-level, which makes for convenient and fast software implementation of AES.

Question 5: Define state in AES? How many states are there in each version of AES?

Solution:

Internally, the AES algorithm's operations are performed on a two-dimensional array of bytes called the State

AES operates on a 4 × 4 column-major order array of bytes, termed as a state.

Four different stages are used, one of permutation and three of substitution:

- ❍ Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block
- ❍ ShiftRows: A simple permutation
- ❍ MixColumns: A substitution that makes use of arithmetic over GF(28)
- ❍ AddRoundKey: A simple bitwise XOR of the current block with a portion of the expanded

Question 6: Which of the four transformations defined for AES change the contents of bytes? Which one does not change the contents of the bytes?

Solution:

AES uses four types of transformations:

- substitution (Sub Bytes)
- permutation(Shift Rows)
- mixing(Mix Columns)
- key-adding(Add Round key)

Substitution:

Substitution is done for each nibble (4-bit data unit). Only one table is used for transformations of every nibble, which means that if two nibbles are the same, the transformation is also the same. In this appendix, transformation is defined by a table lookup process.

Permutation:

Another transformation found in a round is shifting, which permutes the nibbles. Shifting transformation in S-AES is done at the nibble level; the order of the bits in the nibble is not changed.

Mixing:

The mixing transformation changes the contents of each nibble by taking 2 nibbles at a time and combining them to create 2 new nibbles. To guarantee that each new nibble is different (even if the old nibbles are the same

Note: The MixColumns and InvMixColumns transformations are inverses of each other.

Key Adding:

Probably the most important transformation is the one that includes the cipher key. All previous transformations use known algorithms that are invertible. If the cipher key is not added to the state at each round, it is very easy for the adversary to find the plaintext, given the ciphertext. The cipher key is the only secret between Alice and Bob in this case.

Note: The AddRoundKey transformation is the inverse of itself

Question 7: Compare the substitution in DES and AES. Why do we have only one substitution table(S-box) in AES, but several in DES?

Solution:

Substitution in DES :

- After the compressed key is XORed with the expanded block, the 48-bit result moves to a substitution operation.

- Substitutions are performed by eight substitution boxes, or S-boxes.Each box has a 6-bit input and a 4-bit output.

- There are 8 different S-boxes.48-bits are divided into eight 6-bit sub-blocks. Each separate block is operated on by a separate S-box.

- The 6 input bits of the S-box specify under which row and col number to look for the output in S-box table.

Substitution in AES :

- Substitution is done for each byte.

- Substitution in AES involves 16 byte to byte transformations.

- The SubByte transformation repeats a routine, called subbyte, 16 times.

- Only one table is used for transformation of every byte, which means that if two bytes are the same, the transformation is also the

Substitution table in DES and AES :

- We have only one substitution table (S-box) in AES because every byte uses the same table for tansformation and also tansformation is done 1 byte at a time in a state. i.e. if two bytes have the same values , their transformation is also the same.

- In DES uses 8 different S-boxes each with a 6-bit input and a 4-bit output. Because the 48-bit data from second operation is divided into eight 6-bit chunks, and each chunk is fed into a box and result of each box is a 4-bit chunk when combined the result is 32 bit text. each S-box has its own table, so we need eight tables to define the output of these boxes.

Question 8: Compare the permutations in DES and AES. Why do we need expansion and compression permutations in DES, but not in AES?

Solution:

Permutations in DES :

- DES operates on a 64-bit block of plaintext. After an initial permutation , the block is broken into a right half and a left half, each 32 bits long.
- Permutation is done at the bit level.
- The order of the bits is changed.

Permutations in AES :

- It permutes the bytes.
- Permutation is at the byte level.
- The order of the bits in the byte is not changed.
- The transformation is called ShiftRows(encryption) and the shifting is to the left.
- Transformation is one row at a time. The routine shiftraw shifts the byte in a single row. Repeated 3 times for the matrix.
- No .of shifts depends on the row number of the state matrix.
- For decryption the transformation is called InvShiftRows.

Need of Expansion and compression permutations in DES:

** In DES The cipher key size is of 56 bits. The round key size is of 48 bits.

- The block size in DES is 64 bits. Which is divided into two halves 32 bits each.
- The input to the function is a 32-bit word, but the round-key is a 48-bit word. The expansion permutation is needed to increase the number of bits in the Right plain text input word to 48bit.
- Compression permutation is used to select 48 bits out of 56 bits of the shifted key. In other words, shifted key is compressed and permuted at the same time. It is done according to the Compression Permutation table.

Question 9: Compare the round keys in DES and AES. In which cipher is the size of the round key the same as the size of the block?

Solution:

Round keys in DES:

- Each round key is of 48-bits.
- Round key generator creates sixteen 48 bit keys from a 56 bit cipher key.

- There are 16 rounds in DES and each round uses a different 48 bit round key generated from cipher key.

Round keys in AES:

- Each round key is of 128 bits (in all versions of AES).
- The no. of round keys in AES = No. of rounds (Nr) +1 , created using a cipher key.
- No. of round keys is generated by key-expansion algorithm.

**In AES cipher the size of the round key is same as the size of the block.

Question 10: Why do you think the mixing transformation(MixColumns) is not needed in DES, but is needed in AES?

Solution:

IN AES:

The problem in AES is that it uses same single S-box for each byte in the state if all the byte are same then after substitution transformation the contents of each byte will be same. There after it goes to permutation but permutation only changes the order of the bytes not the content. So to resolve this problem mixing transformation is needed.

- In AES the mixing transformation changes the contents of each byte by taking four bytes at a time and combining them to recreate four new bytes. To guarantee that each new byte is different even if all four bytes are the same. That is why we need mixing transformation (Mix Columns) in AES.
- The combination process first multiplies each byte with a different constant and then mixes them. The mixing is provided by matrix multiplication.

IN DES :

- In DES there is not, this kind of problem because it uses 8 –different S-box (tables) which gives 8 different outputs even if all bytes are same in the i