Name: **Shrey Pendurkar**
Class: **D15C**
Batch: **C**
Roll No: **64**

CNS - Experiment 5

AIM: To understand how to Encrypt long messages using various modes of operation using AES and DES

Theory:

DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are two widely used symmetric-key encryption algorithms that serve to protect data confidentiality by converting plaintext data into ciphertext using a secret key. Here's a brief overview of both:

1. DES (Data Encryption Standard):

- Key Length: DES uses a 56-bit encryption key. This relatively short key length is one of the primary reasons why DES is no longer considered secure against modern attacks.

- Block Size: DES operates on 64-bit blocks of plaintext data.

- Encryption Process: DES uses a Feistel network structure. The encryption process involves multiple rounds (typically 16 rounds). During each round, the plaintext block is divided into two halves, and various mathematical operations, including substitution (S-boxes), permutation (P-boxes), and bitwise operations, are applied to each half using a round-specific subkey derived from the main encryption key. The results from each round are mixed and swapped, creating the ciphertext.

- Security Concerns: DES is no longer considered secure against modern cryptographic attacks, primarily due to its short key length. It can be vulnerable to brute-force attacks where an attacker tries all possible 2^56 keys to decrypt the data.

2. AES (Advanced Encryption Standard):

- Key Length: AES supports multiple key lengths, including 128-bit, 192-bit, and 256-bit keys. Longer key lengths provide higher security.
- Block Size:AES operates on 128-bit blocks of plaintext data.
- Encryption Process: AES uses a substitution-permutation network (SPN) structure. The encryption process involves several rounds, with the number of rounds depending on the key length (10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys). Each round consists of several operations, including a substitution step (SubBytes), permutation step (ShiftRows), mixing step (MixColumns), and adding a round key (XOR with a round-specific key derived from the main encryption key).
- Security: AES is widely regarded as highly secure against both brute-force and cryptographic attacks when used with sufficient key lengths. It has withstood extensive scrutiny and is widely adopted in various applications, including data encryption, secure communication protocols, and more.

1. Define confusion and diffusion. Give examples from DES and AES.

In cryptography, **confusion** and **diffusion** are two fundamental principles that help secure encrypted data.

- **Confusion** makes the relationship between the ciphertext and the key as complex as possible, preventing attackers from deducing the key, even if parts of the ciphertext are known.
- **Diffusion** spreads the influence of a single plaintext bit over many ciphertext bits, hiding patterns in the input data.

Examples:

- **DES:**
  - *Confusion:* Achieved through the use of 8 S-boxes in each of the 16 rounds. Each S-box maps 6 input bits to 4 output bits in a non-linear way.

    - *Diffusion:* Achieved by expansion, permutation, and bit swapping during the Feistel rounds. Each round modifies the data in a way that spreads bits across the block.
- **AES:**
    - *Confusion:* Provided by the **SubBytes** step, where each byte is replaced using a non-linear S-box.
    - *Diffusion:* Achieved through **ShiftRows** (shifting bytes within rows) and **MixColumns** (combining bytes within columns), which ensure that a small change in the input affects many bits in the output.

2. Describe the key expansion process for DES and AES. How does key size affect AES rounds?

Both DES and AES use key expansion to generate round keys from the main encryption key.

- **DES Key Expansion:**
    - Uses a 56-bit key (from the original 64-bit input; 8 bits are parity).
    - Generates 16 subkeys, each 48 bits long, using **permutations** and **left shifts**.
    - Each subkey is used in one of the 16 rounds.
- **AES Key Expansion:**
    - AES supports key sizes of 128, 192, and 256 bits.
    - Key expansion involves:
        - **RotWord** (rotates words),
        - **SubWord** (applies S-box),
        - **Rcon** (round constants),
        - and XOR operations.
    - Number of rounds depends on key size:
        - 128-bit key → **10 rounds**
        - 192-bit key → **12 rounds**
        - 256-bit key → **14 rounds**
    - Each round uses a unique key derived from the expanded key schedule.

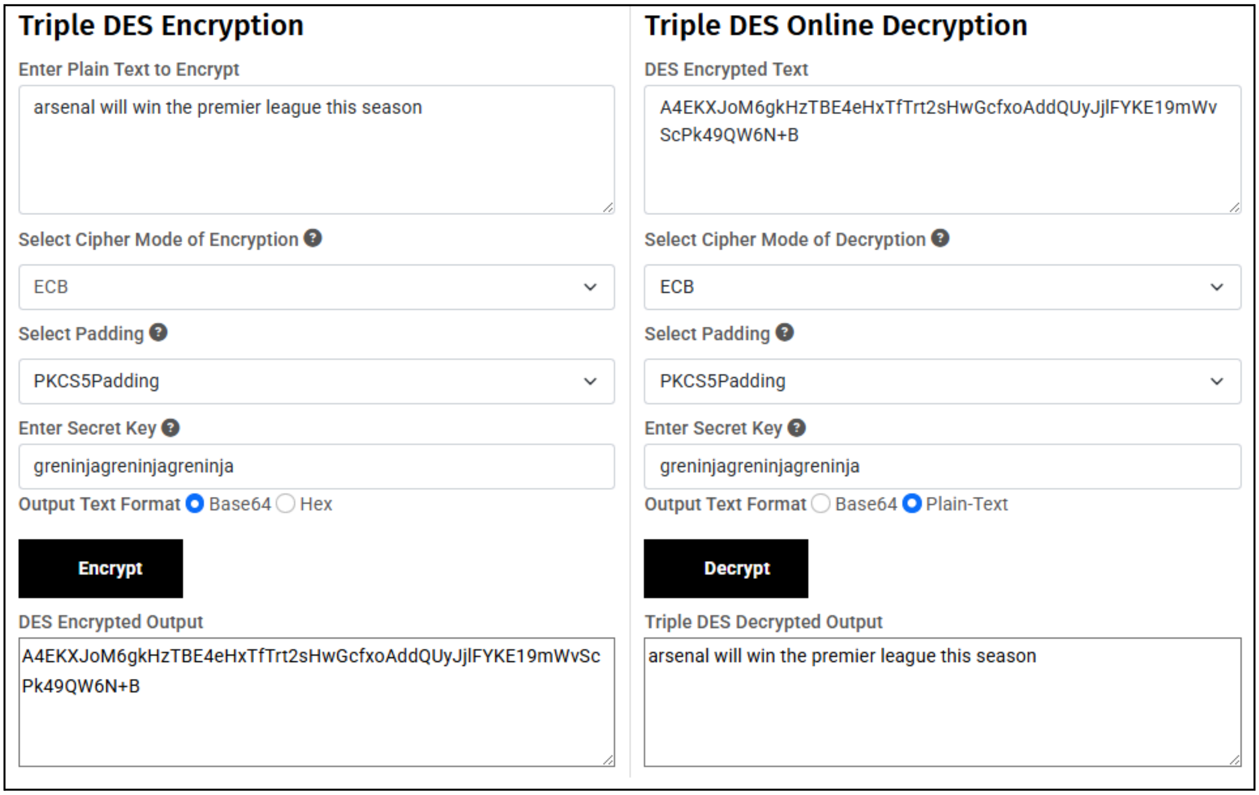
3. What is the importance of Initialization Vector (IV) and CTR mode?

- **Initialization Vector (IV):**
    - A random or unique value used in encryption modes like CBC, OFB, or CTR.
    - Ensures that encrypting the same plaintext with the same key produces different ciphertexts.
    - Prevents attackers from detecting patterns or repetitions in encrypted data.
- **CTR (Counter Mode):**
    - Converts a block cipher into a stream cipher.
    - Uses a counter (usually combined with an IV) to generate a keystream, which is XORed with plaintext.
    - **Advantages:**
        - Allows **parallel encryption** of blocks.
        - Each block uses a different counter value, ensuring uniqueness.
        - Supports random access (good for files or streaming).
        - Safer against block pattern analysis than ECB or CBC.

4. Compare the computational complexity of DES and AES. Which is more resource-intensive and why?

- **DES:**
    - Simpler algorithm with only 16 rounds.
    - Operates on 64-bit blocks and uses a 56-bit key.
    - Faster and less resource-intensive, but also **much less secure**.
    - Vulnerable to brute-force attacks due to small key space.
- **AES:**
    - More complex algorithm with 10–14 rounds (depending on key size).
    - Operates on 128-bit blocks and supports 128/192/256-bit keys.
    - Involves more mathematical operations (S-boxes, matrix multiplication in MixColumns, etc.).
    - **More resource-intensive** in terms of CPU and memory but offers **much higher security**.

Conclusion:
While DES is faster and uses fewer resources, it is outdated and insecure. AES, though more computationally demanding, is the modern standard due to its strong security and flexibility.



Triple DES Encryption

Enter Plain Text to Encrypt

arsenal will win the premier league this season

Select Cipher Mode of Encryption ❓

ECB

Select Padding ❓

PKCS5Padding

Enter Secret Key ❓

greninjagreninjagreninja

Output Text Format ● Base64 ○ Hex

DES Encrypted Output

A4EKXJoM6gkHzTBE4eHxTfTrt2sHwGcfxoAddQUyJjlFYKE19mWvScPk49QW6N+B

Triple DES Online Decryption

DES Encrypted Text

A4EKXJoM6gkHzTBE4eHxTfTrt2sHwGcfxoAddQUyJjlFYKE19mWvScPk49QW6N+B

Select Cipher Mode of Decryption ❓

ECB

Select Padding ❓

PKCS5Padding

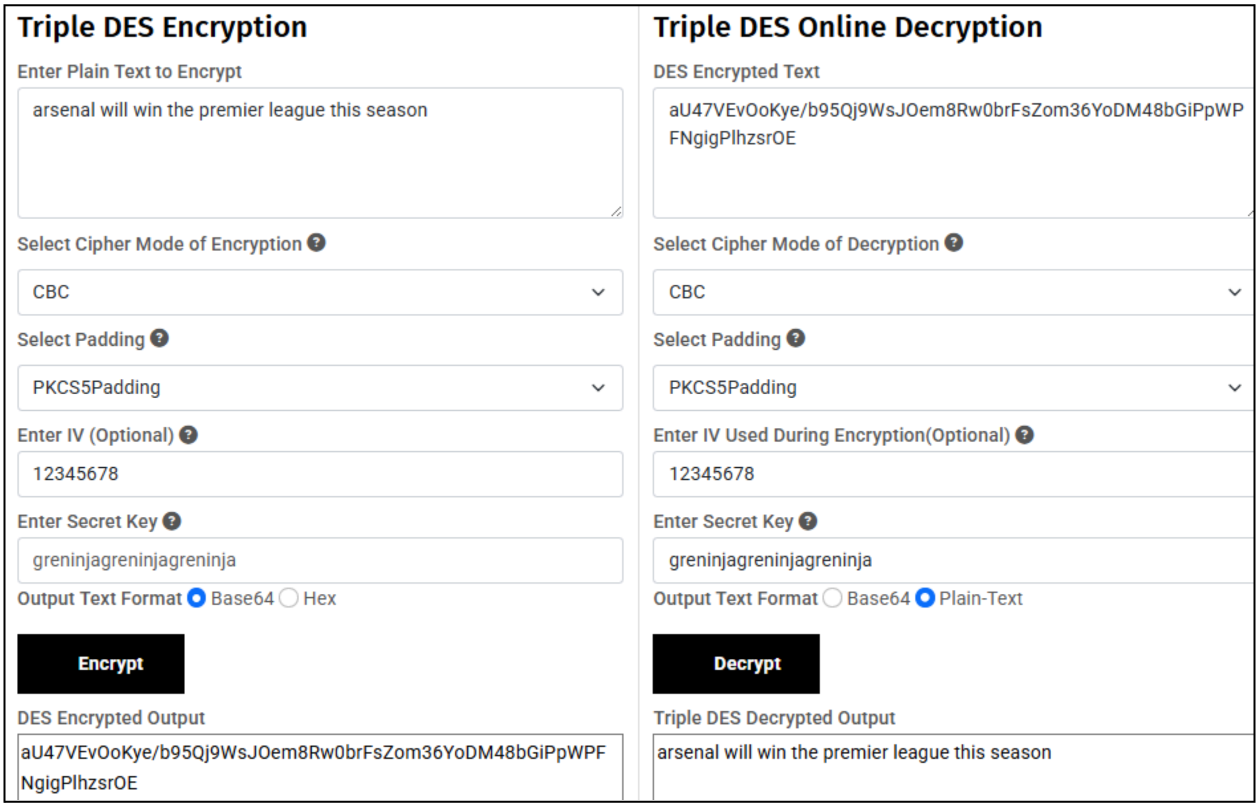
Enter Secret Key ❓

greninjagreninjagreninja

Output Text Format ○ Base64 ● Plain-Text

Triple DES Decrypted Output

arsenal will win the premier league this season



Triple DES Encryption

Enter Plain Text to Encrypt

arsenal will win the premier league this season

Select Cipher Mode of Encryption ❓

CBC

Select Padding ❓

PKCS5Padding

Enter IV (Optional) ❓

12345678

Enter Secret Key ❓

greninjagreninjagreninja

Output Text Format ● Base64 ○ Hex

DES Encrypted Output

aU47VEvOoKye/b95Qj9WsJOem8Rw0brFsZom36YoDM48bGiPpWPFNgigPlhzsrOE

Triple DES Online Decryption

DES Encrypted Text

aU47VEvOoKye/b95Qj9WsJOem8Rw0brFsZom36YoDM48bGiPpWPFNgigPlhzsrOE

Select Cipher Mode of Decryption ❓

CBC

Select Padding ❓

PKCS5Padding

Enter IV Used During Encryption(Optional) ❓

12345678

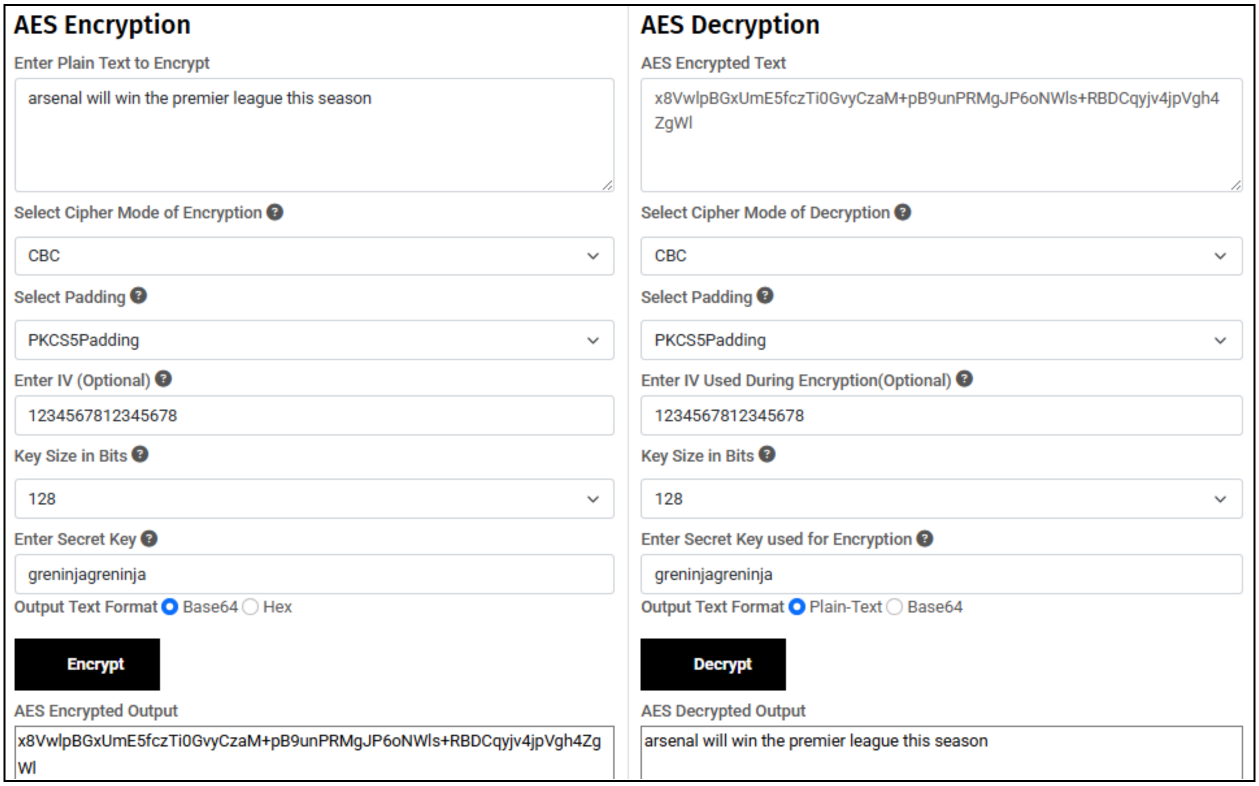
Enter Secret Key ❓

greninjagreninjagreninja

Output Text Format ○ Base64 ● Plain-Text

Triple DES Decrypted Output

arsenal will win the premier league this season



AES Encryption

Enter Plain Text to Encrypt

arsenal will win the premier league this season

Select Cipher Mode of Encryption

CBC

Select Padding

PKCS5Padding

Enter IV (Optional)

1234567812345678

Key Size in Bits

128

Enter Secret Key

greninjagreninja

Output Text Format ● Base64 ○ Hex

AES Encrypted Output

x8VwlpBGxUmE5fczTi0GvyCzaM+pB9unPRMgJP6oNWls+RBDCqyjv4jpVgh4ZgWl

AES Decryption

AES Encrypted Text

x8VwlpBGxUmE5fczTi0GvyCzaM+pB9unPRMgJP6oNWls+RBDCqyjv4jpVgh4ZgWl

Select Cipher Mode of Decryption

CBC

Select Padding

PKCS5Padding

Enter IV Used During Encryption(Optional)

1234567812345678

Key Size in Bits

128

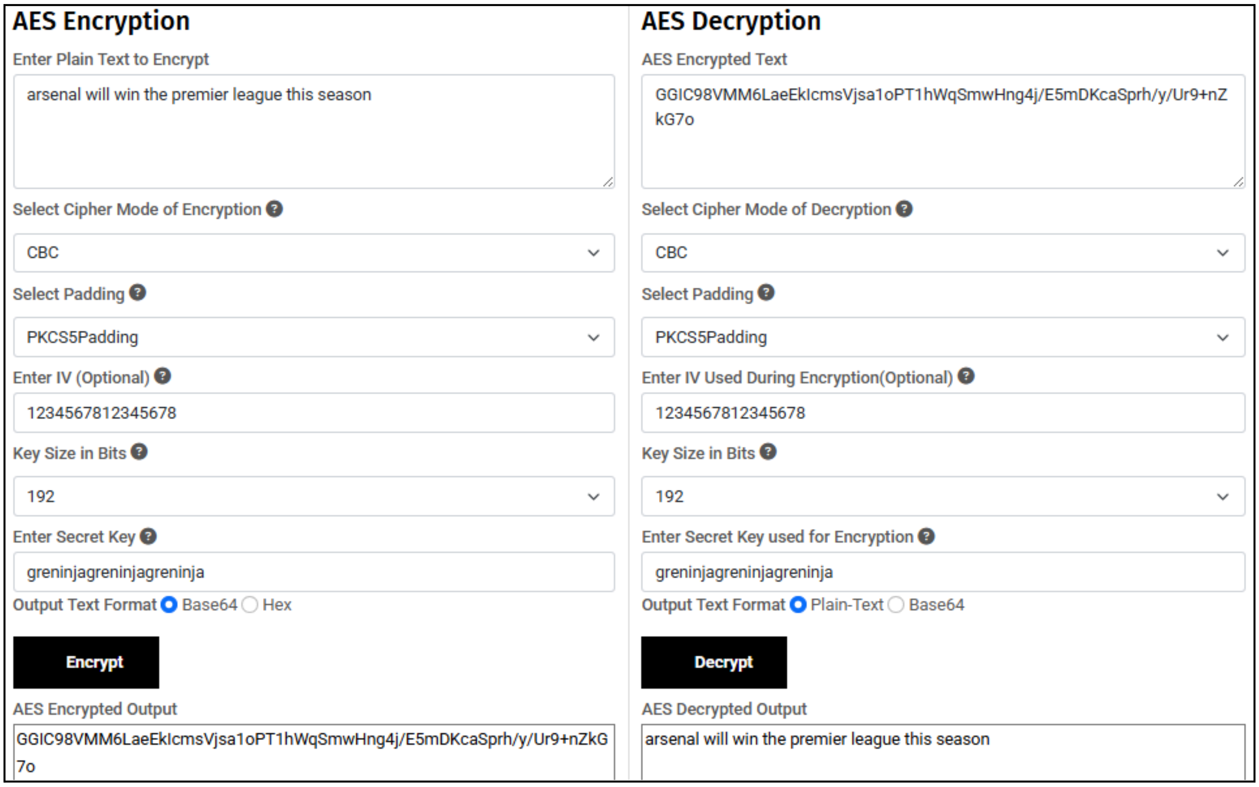
Enter Secret Key used for Encryption

greninjagreninja

Output Text Format ● Plain-Text ○ Base64

AES Decrypted Output

arsenal will win the premier league this season



AES Encryption

Enter Plain Text to Encrypt

arsenal will win the premier league this season

Select Cipher Mode of Encryption

CBC

Select Padding

PKCS5Padding

Enter IV (Optional)

1234567812345678

Key Size in Bits

192

Enter Secret Key

greninjagreninjagreninja

Output Text Format ● Base64 ○ Hex

AES Encrypted Output

GGIC98VMM6LaeEkIcmsVjsa1oPT1hWqSmwHng4j/E5mDKcaSprh/y/Ur9+nZkG7o

AES Decryption

AES Encrypted Text

GGIC98VMM6LaeEkIcmsVjsa1oPT1hWqSmwHng4j/E5mDKcaSprh/y/Ur9+nZkG7o

Select Cipher Mode of Decryption

CBC

Select Padding

PKCS5Padding

Enter IV Used During Encryption(Optional)

1234567812345678

Key Size in Bits

192

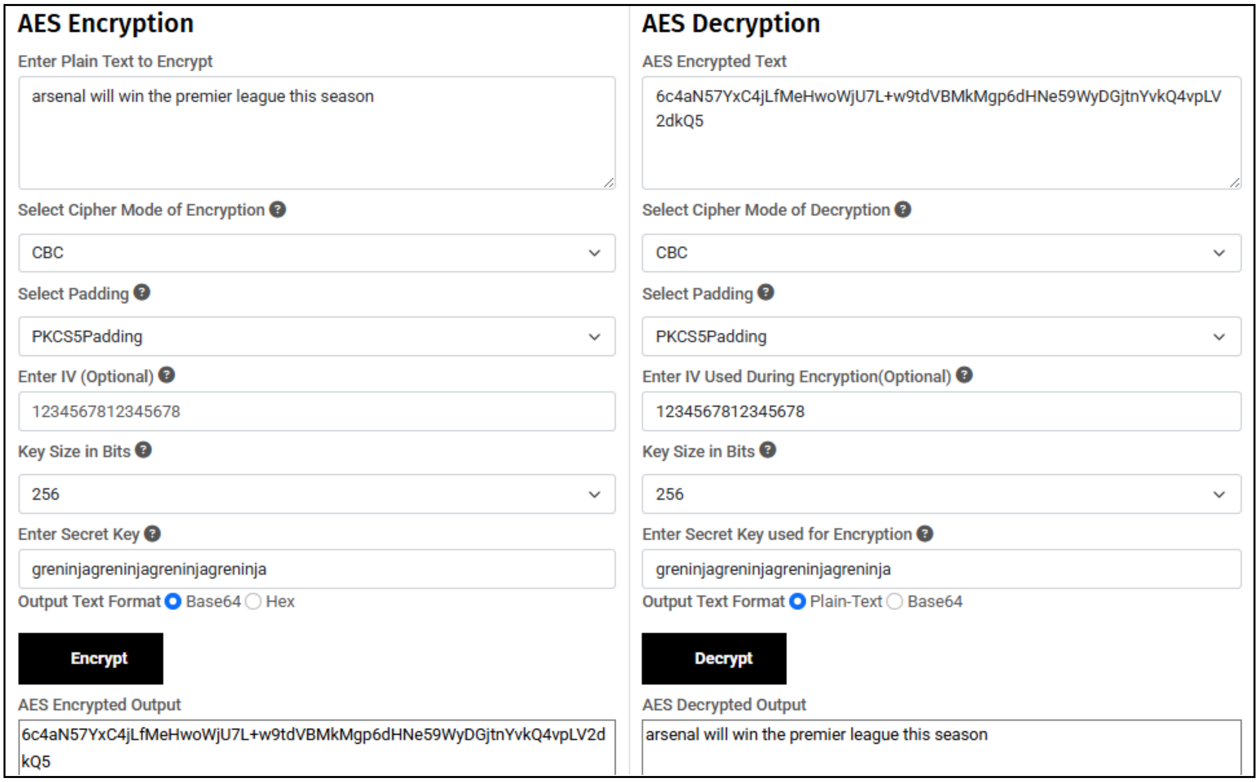
Enter Secret Key used for Encryption

greninjagreninjagreninja

Output Text Format ● Plain-Text ○ Base64

AES Decrypted Output

arsenal will win the premier league this season



AES Encryption

Enter Plain Text to Encrypt

arsenal will win the premier league this season

Select Cipher Mode of Encryption: CBC

Select Padding: PKCS5Padding

Enter IV (Optional): 1234567812345678

Key Size in Bits: 256

Enter Secret Key: greninjagreninjagreninjagreninja

Output Text Format ● Base64 ○ Hex

AES Encrypted Output

```
6c4aN57YxC4jLfMeHwoWjU7L+w9tdVBMkMgp6dHNe59WyDGjtnYvkQ4vpLV2dkQ5
```

AES Decryption

AES Encrypted Text

```
6c4aN57YxC4jLfMeHwoWjU7L+w9tdVBMkMgp6dHNe59WyDGjtnYvkQ4vpLV2dkQ5
```

Select Cipher Mode of Decryption: CBC

Select Padding: PKCS5Padding

Enter IV Used During Encryption(Optional): 1234567812345678

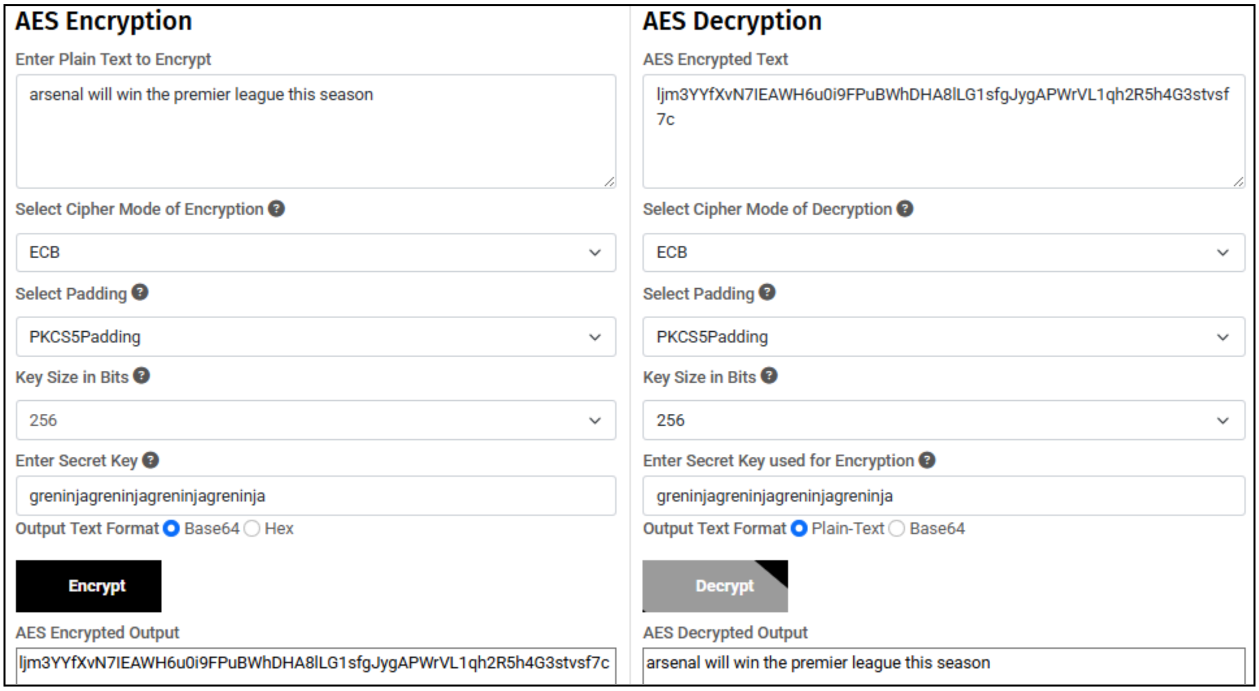
Key Size in Bits: 256

Enter Secret Key used for Encryption: greninjagreninjagreninjagreninja

Output Text Format ● Plain-Text ○ Base64

AES Decrypted Output

arsenal will win the premier league this season



AES Encryption

Enter Plain Text to Encrypt

arsenal will win the premier league this season

Select Cipher Mode of Encryption: ECB

Select Padding: PKCS5Padding

Key Size in Bits: 256

Enter Secret Key: greninjagreninjagreninjagreninja

Output Text Format ● Base64 ○ Hex

AES Encrypted Output

```
ljm3YYfXvN7IEAWH6u0i9FPuBWhDHA8lLG1sfgJygAPWrVL1qh2R5h4G3stvsf7c
```

AES Decryption

AES Encrypted Text

```
ljm3YYfXvN7IEAWH6u0i9FPuBWhDHA8lLG1sfgJygAPWrVL1qh2R5h4G3stvsf7c
```

Select Cipher Mode of Decryption: ECB

Select Padding: PKCS5Padding

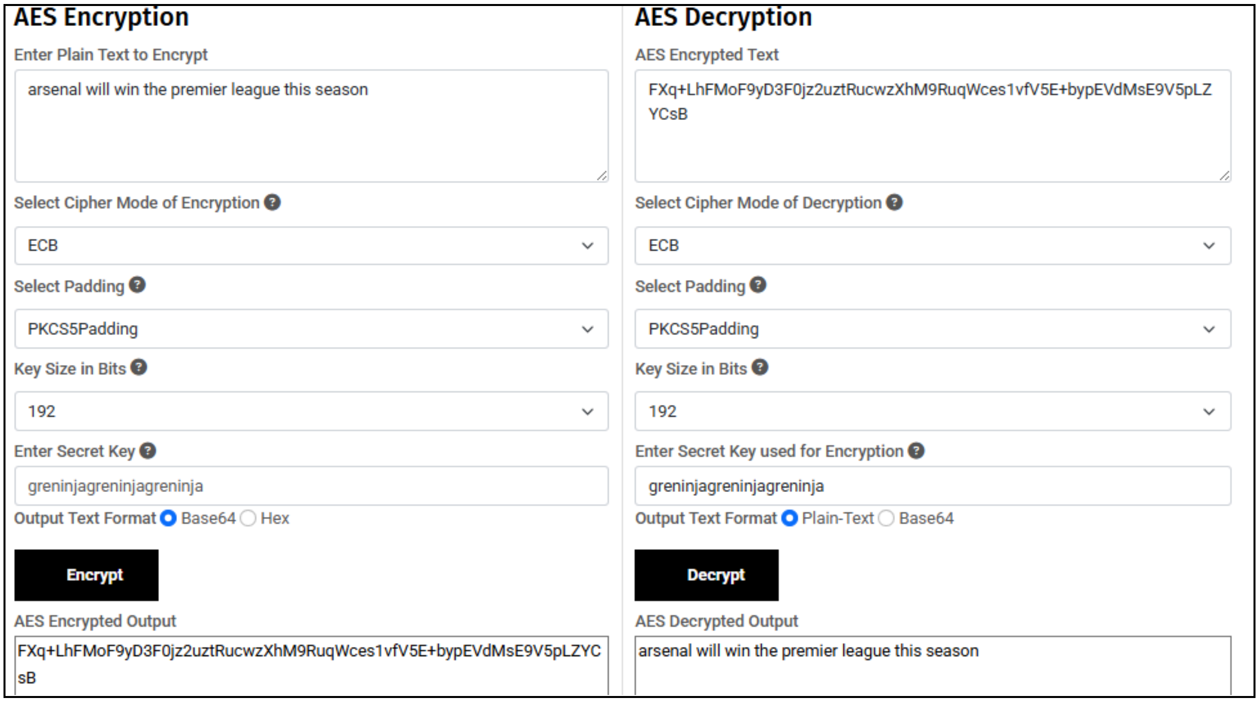
Key Size in Bits: 256

Enter Secret Key used for Encryption: greninjagreninjagreninjagreninja

Output Text Format ● Plain-Text ○ Base64

AES Decrypted Output

arsenal will win the premier league this season



AES Encryption

Enter Plain Text to Encrypt

arsenal will win the premier league this season

Select Cipher Mode of Encryption: ECB

Select Padding: PKCS5Padding

Key Size in Bits: 192

Enter Secret Key: greninjagreninjagreninja

Output Text Format ● Base64 ○ Hex

AES Encrypted Output

FXq+LhFMoF9yD3F0jz2uztRucwzXhM9RuqWces1vfV5E+bypEVdMsE9V5pLZYCsB

AES Decryption

AES Encrypted Text

FXq+LhFMoF9yD3F0jz2uztRucwzXhM9RuqWces1vfV5E+bypEVdMsE9V5pLZYCsB

Select Cipher Mode of Decryption: ECB

Select Padding: PKCS5Padding

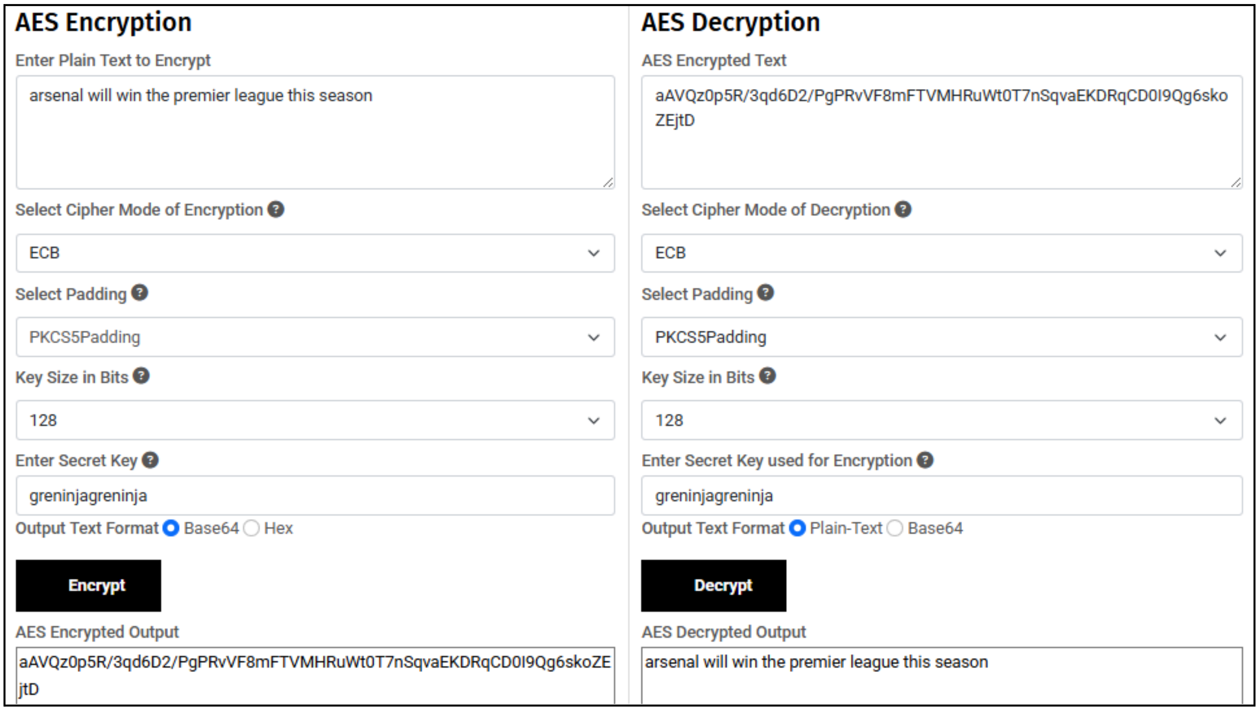
Key Size in Bits: 192

Enter Secret Key used for Encryption: greninjagreninjagreninja

Output Text Format ● Plain-Text ○ Base64

AES Decrypted Output

arsenal will win the premier league this season



AES Encryption

Enter Plain Text to Encrypt

arsenal will win the premier league this season

Select Cipher Mode of Encryption: ECB

Select Padding: PKCS5Padding

Key Size in Bits: 128

Enter Secret Key: greninjagreninja

Output Text Format ● Base64 ○ Hex

AES Encrypted Output

aAVQz0p5R/3qd6D2/PgPRvVF8mFTVMHRuWt0T7nSqvaEKDRqCD0I9Qg6skoZEjtD

AES Decryption

AES Encrypted Text

aAVQz0p5R/3qd6D2/PgPRvVF8mFTVMHRuWt0T7nSqvaEKDRqCD0I9Qg6skoZEjtD

Select Cipher Mode of Decryption: ECB

Select Padding: PKCS5Padding

Key Size in Bits: 128

Enter Secret Key used for Encryption: greninjagreninja

Output Text Format ● Plain-Text ○ Base64

AES Decrypted Output

arsenal will win the premier league this season