Decrypting morse code: S3CR3TK3Y@123456

To decrypt the ciphertext "hoZyGgMHU4dM+8zgZAPXhA==" using the key "S3CR3TK3Y@123456", we'll use the AES (Advanced Encryption Standard) algorithm

**1. Ciphertext Encoding and Decoding**

* **Ciphertext Encoding**: The ciphertext is given in Base64 encoding, which is a way to represent binary data as text. Base64 is used to make binary data (which might include non-printable characters) safe to transmit over text-based protocols.
* **Base64 Decoding**: Convert the Base64 encoded ciphertext back into its original binary format. This is the raw data that will be decrypted.

**2. AES Algorithm**

* **AES Overview**: AES is a symmetric key encryption algorithm. It encrypts and decrypts data using the same key. AES operates on blocks of data (128 bits at a time) and supports key sizes of 128, 192, or 256 bits.
* **Key Size**: The provided key "S3CR3TK3Y@123456" is 16 bytes long (128 bits), which means we are using AES-128. AES-128 uses a key size of 128 bits.

**3. AES Mode of Operation**

* **ECB Mode**: In Electronic Codebook (ECB) mode, each block of plaintext is encrypted independently. While simple, ECB mode is not recommended for most applications due to its security weaknesses (it doesn’t hide data patterns). It is used here for simplicity based on your context.

**4. Decryption Process**

1. **Initialize the AES Cipher**: Create an AES cipher object using the provided key and specify the mode of operation (in this case, ECB mode).
2. **Decrypt the Ciphertext**: Use the AES cipher object to decrypt the binary data obtained from Base64 decoding.
3. **Remove Padding**: If padding was added during encryption to make the plaintext a multiple of the block size, it needs to be removed. AES encryption typically uses padding schemes like PKCS7. If padding is not used or if the ciphertext doesn't require padding, this step can be skipped.
4. **Obtain Plaintext**: The result of the decryption operation should be the original plaintext before encryption.

The password is: algorithmissafe

The Secret code present in the Cyber Threat Advanced Machine Learning Algorithm PDF: CogML24@2024