AES Algorithm 128

Advanced Encryption Standard , presently the much popular method of encrypting the transactions. It can roughly be considered to be an advanced version of the earlier secret key system called DES, D standing for data. All the confusion and diffusion functions of DES are taken to a hyper level , like the each round variable S-Box structure.The ultimate aim being to make the AES code breaking in feasible.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

It makes sense to understand stream and block ciphers first. Then, have a look at the simple differences between symmetric and asymmetric ciphers.

It's worth knowing the historical background of AES. Why DES wasn't secure enough? Why people needed something else? What NSA knew before everyone else?

If you want to know more about NSA and AES relation can share a story buut its an assignment so end it here only

CODE:

```
import java.io.UnsupportedEncodingException;
```

```
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.util.Arrays;
import java.util.Base64;

import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;

public class AES {

	private static SecretKeySpec secretKey;
	private static byte[] key;

	public static void setKey(String myKey)
	{
		MessageDigest sha = null;
		try {
			key = myKey.getBytes("UTF-8");
			sha = MessageDigest.getInstance("SHA-1");
			key = sha.digest(key);
			key = Arrays.copyOf(key, 16);
			secretKey = new SecretKeySpec(key, "AES");
		}
		catch (NoSuchAlgorithmException e) {
			e.printStackTrace();
		}
		catch (UnsupportedEncodingException e) {
			e.printStackTrace();
		}
	}

	public static String encrypt(String strToEncrypt, String secret)
	{
		try
		{
			setKey(secret);
			Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
			cipher.init(Cipher.ENCRYPT_MODE, secretKey);
			return
Base64.getEncoder().encodeToString(cipher.doFinal(strToEncrypt.getBytes("UTF-8")));
		}
		catch (Exception e)
		{
			System.out.println("Error while encrypting: " + e.toString());
		}
		return null;
	}




public static void main(String[] args)
{
	final String secretKey = "asdfghjklpoiuytr";

	String originalString = "Good morning Mam";
	String encryptedString = AES.encrypt(originalString, secretKey) ;
```

```
        System.out.println(originalString);
        System.out.println(encryptedString);

}
```

Terminal: