Dumpster

Dumpster

I found a flag, but it was encrypted!
Our systems have detected that someone has successfully decrypted this flag, and we stealthily took a heap dump of the program (in Java).
Can you recover the flag for me?
Here's the source code of the Java program and the heap dump:

https://mega.nz/#!rHYGlAQT!48DlH2pSZg10Ei3f-Ivm7RoNBbV16Qw0wN4cWxANUwY

Flag: CTFlearn{h34p_6ump5_r_c00l!11!!}

Writeup:

Opened dump file in visualvm and found the passHash thread
then wrote java program to decrypt hash:

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

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

public class Decryptor
{
	public static final String FLAG = "S+kUZtaHEYpFpv2ixuTnqBdORNzsdVJrAxWznyOljEo=";

	public static byte[] decrypt(byte[] msg, byte [] passHash) throws Exception
	{
		SecretKeySpec spec = new SecretKeySpec(passHash, "AES");
		Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
		cipher.init(Cipher.DECRYPT_MODE, spec);
		return cipher.doFinal(msg);
	}

	public static void main(String[] args) throws Exception
	{
		byte[] passHash = {7, 95, -34, 16, -89, -86, 73, 108, -128, 71, 43, 41, 100, 40, 53, -24};
		System.out.println(new String(decrypt(Base64.getDecoder().decode(FLAG.getBytes()),passHash)));
	}
}
```

ran java script and got flag

stCTF{h34p_6ump5_r_c00l!11!!}