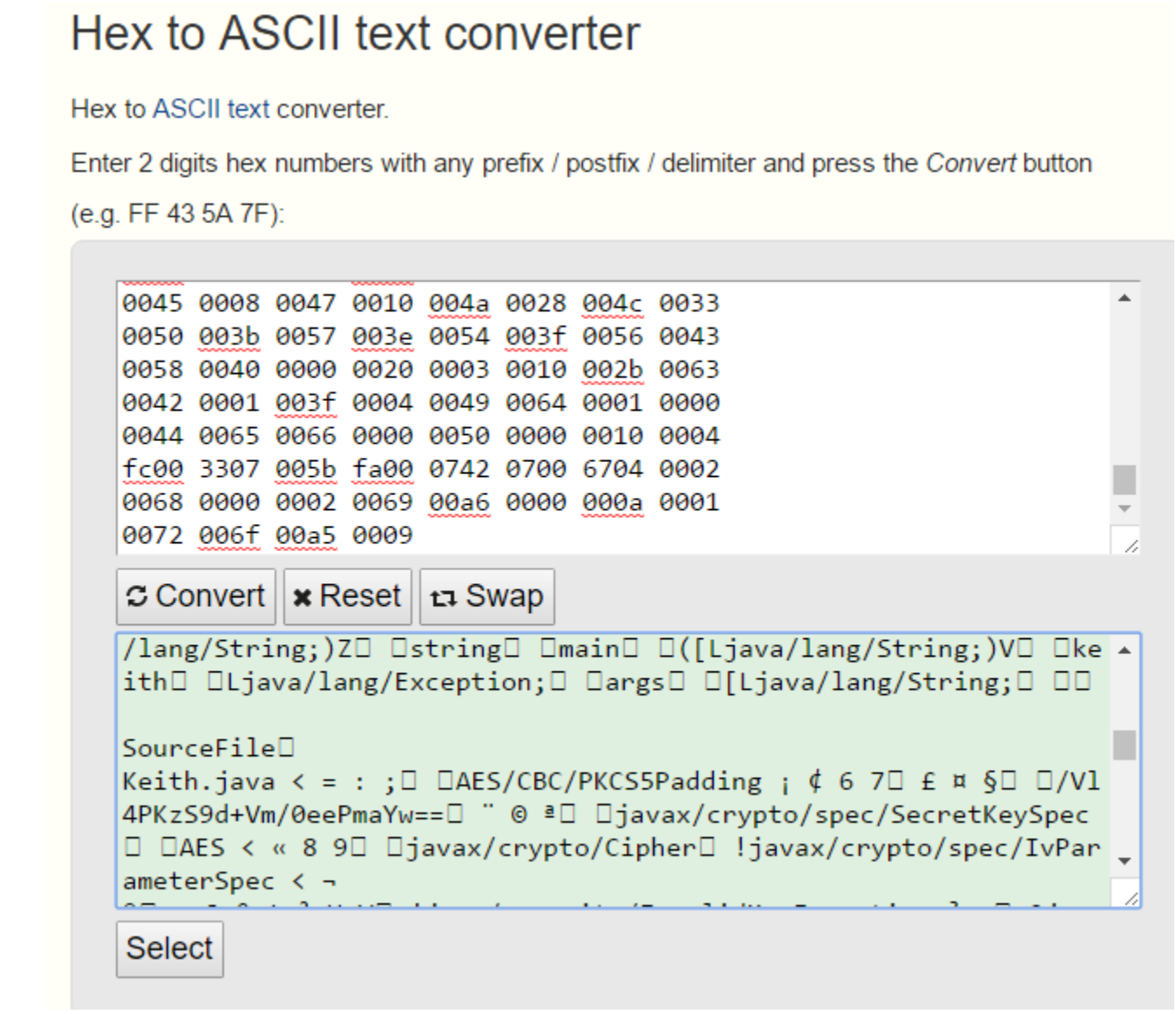
1.KE1TH – 200pt (Trần Thanh Tuấn):

- Download file về, ta có 1 file binary gì đó đọc chả hiểu, thử convert qua ascii xem:



- Ồ thì ra đây là 1 file java đã được complie, xài Java Decompiler ta có được mã nguồn gốc, để ý trên mã nguồn gốc, đây là kết quả cuối cùng của flag đã bị mã hóa, ta cần giải mã cái này:

```
public boolean check(String string)
{
  return string.equals("-93^35^23^82^-4^57^-128^83^-95^-60^-100^73^40^-86^7^73^-101^3^118^-66^-104^69^121^76^1^-124^-124^-1^-64^29^28^43^2^-25
  ^54^52^-79^-62^11^-43^52^-72^-117^-25^-103^-55^75^-97^");
}
```

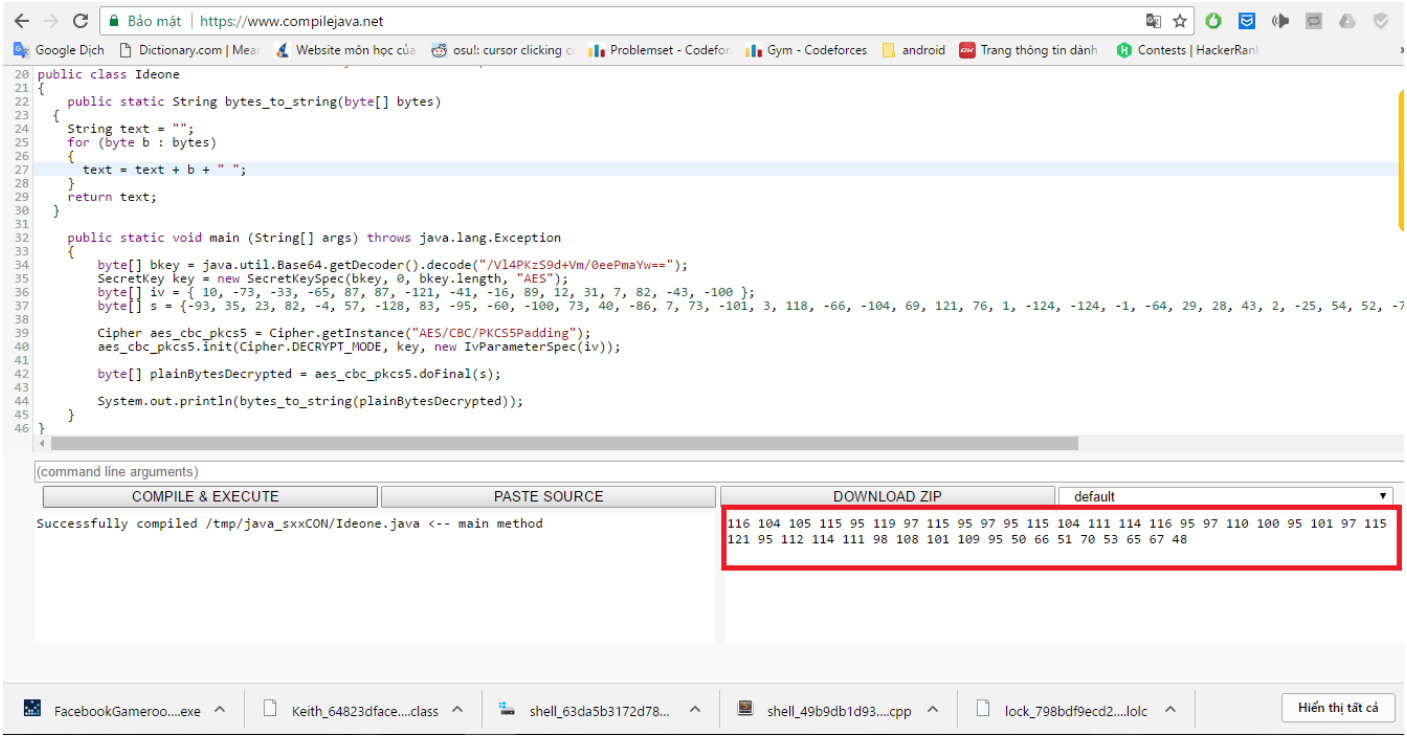
- Còn đây là phần mã hóa:

```
public Keith() throws javax.crypto.NoSuchPaddingException, NoSuchAlgorithmException, InvalidAlgorithmParameterException, InvalidKeyException
{
  aes_cbc_pkcs5 = Cipher.getInstance("AES/CBC/PKCS5Padding");

  byte[] bkey = java.util.Base64.getDecoder().decode("/Vl4PKzS9d+Vm/0eePmaYw==");
  key = new SecretKeySpec(bkey, 0, bkey.length, "AES");
}

public String encrypt(String plain)
{
  try {
    aes_cbc_pkcs5.init(1, key, new IvParameterSpec(iv));
    return bytes_to_string(aes_cbc_pkcs5.doFinal(plain.getBytes()));
  }
```

- Tới bước này thì đơn giản rồi, ta tách cái chuỗi kết quả mã hóa cuối cùng ra thành dãy byte (bỏ đấu ^ đi), sau đó viết code java dùng cipher decrypt ngược lại cái dãy byte đó là ra dãy byte ban đầu của flag:



- Dùng convert từ byte sang ascii ta có được flag :

ASCII Converter - Hex, decimal, binary, and ASCII converter

Convert ASCII (Example: a b c)

```
t h i s _ w a s _ a _ s h o r t _ a n d _ e a s y _ p r o b l e m _ 2 B 3 F 5 A C 0
```

Add spaces | Remove spaces | Convert white space characters

Convert Hex (Example: 0x61 0x62 0x63) Remove 0x

```
0x74 0x68 0x69 0x73 0x5f 0x77 0x61 0x73 0x5f 0x61 0x5f 0x73 0x68 0x6f 0x72 0x74
0x5f 0x61 0x6e 0x64 0x5f 0x65 0x61 0x73 0x79 0x5f 0x70 0x72 0x6f 0x62 0x6c 0x65
0x6d 0x5f 0x32 0x42 0x33 0x46 0x35 0x41 0x43 0x30
```

Convert Decimal (Example: 97 98 99)

```
116 104 105 115 95 119 97 115 95 97 95 115 104 111 114 116 95 97 110 100 95 101 97
115 121 95 112 114 111 98 108 101 109 95 50 66 51 70 53 65 67 48
```

- Flag: “this_was_a_short_and_easy_problem_2B3F5AC0”