NOTE: SCENARIO IS WHAT PUZZLE TAKER SEES.

SCENARIO:

See the J23-Cipher.getOutputSize puzzle.

```
01   // OMITTED: Import whatever is needed.
02   public final class CryptoUtils {
03     public static byte[] encrypt (String alg, Key key, String text)
04         throws GeneralSecurityException {
05       // Create a cipher
06       Cipher cipher = Cipher.getInstance(alg);
07       cipher.init(Cipher.ENCRYPT_MODE, key);
08
09       // Encrypt the data
10       byte[] input = text.getBytes();
11       byte[] output = new byte[cipher.getOutputSize(input.length)];
12
13       int length = cipher.update(input, 0, input.length, output, 0);
14       length += cipher.doFinal(output, length);
15       return output;
16     }
17   }
```

Questions:
See the J23-Cipher.getOutputSize puzzle.

NOTE: ANSWER IS TO BE SHOWN TO PUZZLE TAKER AT THE END OF SESSION.

ANSWER:
d
See the J23-Cipher.getOutputSize puzzle.

NOTE: THE REST OF DOCUMENT CONTAINS EXTRA INFORMATION FOR THE PROJECT RESEARCHERS. IT IS NOT TO BE SHOWN TO PUZZLE TAKERS.

TAGS:
java, cryptography, cipher, invalid-object-initialization, api-protocol-usage, non-security-blindspot

CATEGORIES:
Blindspot - NO
Type - Crypto

Number of distinct functions - 7
Number of total functions - 7
Blindspot function - NA
Function call omitted - NA
Blindspot type - NA
Number of Parameters in the blindspot function - NA
Cyclomatic complexity - 2

NAME:
Cipher class, getOutputSize method - Provides the functionality of a cryptographic cipher for encryption and decryption. It forms the core of the Java Cryptographic Extension (JCE) framework.

MORE INFORMATION:
To see a vulnerable way of use of the API look at the J23-Cipher.getOutputSize puzzle.

REFERENCES:
1. Cipher