Applied Cryptography
Quiz Demo

April 3, 2025

1. Given a padded string, determine which type of padding has been used?

   (a) `hello/x0b/x0b/x0b/x0b/x0b/x0b/x0b/x0b/x0b/x0b/x0b`:

   - ☐ PKCS7
   - ☐ ISO7816
   - ☐ x923

   (b) `helloworld!/x80/x00/x00/x00/x00`:

   - ☐ PKCS7
   - ☐ ISO7816
   - ☐ x923

   (c) `thisisnotpadding/x10/x10/x10/x10/x10/x10/x10/x10/x10/x10/x10/x10/x10/x10/x10/x10`:

   - ☐ PKCS7
   - ☐ ISO7816
   - ☐ x923

[3 points]

2. Read the following code.

```python
from cryptography.hazmat.primitives.ciphers.algorithms import AES
from cryptography.hazmat.primitives.ciphers import modes, Cipher
from cryptography.hazmat.primitives import padding
import os

def encrypt(message, key):
    iv = os.urandom(16)
    padder = padding.PKCS7(AES.block_size).padder()
    cipher = Cipher(AES(key), modes.CBC(iv))
    encryptor = cipher.encryptor()
    ciphertext = encryptor.update(padder.update(message)+padder.finalize()) + encryptor
    .finalize()
    return ciphertext

message = os.urandom(30)
key = os.urandom(16)

print(encrypt(message, key))
```

   (a) Describe what it is doing.

[4 points]

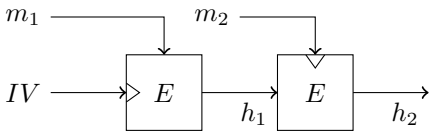
3. Draw the Encrypt-then-MAC strategy?

[4 points]

4. Draw the ECB Mode and describe its weaknesses.

[4 points]

5. Consider the following hash function $H : \{0,1\}^{2n} \mapsto \{0,1\}^n$, where E is a block cipher (meaning that you can compute the inverse if you know the key). The key is highlighted by the $\wedge$ symbol (accordingly oriented). Can you find a collision (a message different from $m1||m2$ such that the resulting hash is the same)?



[5 points]

6. Use formulas and drawings to describe how you can use the CBC padding oracle attack to obtain the last byte of the plaintext.

[5 points]