Assignment 1 – 2019.09.17

Submission Deadline: 2019.09.25 (Before Lab Tutorial)

1. Let $G:\{0,1\}^s \rightarrow \{0,1\}^n$ be a secure PRG. Which of the following is a secure PRG (could be more than one), and give your explanation.

$G'(k_1,k_2) = G(k_1)||G(k_2)$
$G'(k) = G(0)$
$G'(k) = G(k)$
$G'(k) = G(k)||0$
$G'(k) = G(k \oplus 1^s)$
$G'(k) = reserver(G(k))$, where reverse(x) reverses the string x so that the first bit of x is the last bit of reverse(x) and so on.

2. Let $G:K \rightarrow \{0,1\}^n$ be a secure PRG. Define $G'(k_1,k_2) = G(k_1) \wedge G(k_2)$ where $\wedge$ is the **bit-wise AND function**. Consider the following statistical test A on $\{0,1\}^n$. A(x) outputs LSB(x), the least significant bit of x. What is the Adv_{PRG}[A,G']? You may assume that LSB(G(k)) is 0 for exactly half the seeds k in K.

3. Let (E, D) be a one-time semantically secure cipher where the message and ciphertext space is $\{0,1\}^n$. Which of the following encryption scheme are semantically secure? Give your explanation for each of the options.

1) $E'\big((k,k'),m\big) = E(k,m)||E(k',m\ )$
2) $E'(k,m\ ) = E(0^n,m)$
3) $E'(k,m\ ) = E(k,m)||k$
4) $E'(k,m\ ) = E(k,m)||LSB(m)$

4. Suppose you are told that the one time pad encryption of the message "attack at dawn" is 6c73d5240a948c86981bc294814d (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex). What would be the one time pad encryption of the message "attack at dusk" under the same OTP key?

5. Let us see what goes wrong when a stream cipher key is used more than once. Below are eleven hex-encoded ciphertexts that are the result of encrypting eleven plaintexts with a stream cipher, all

with the same stream cipher key. Your goal is to decrypt the last ciphertext, and submit the secret message within it as solution.

Hint: XOR the ciphertexts together, and consider what happens when a space is XORed with a character in [a-zA-Z].

ciphertext #1:

```
315c4eeaa8b5f8aaf9174145bf43e1784b8fa00dc71d885a804e5ee9fa40b16349c14
6fb778cdf2d3aff021dfff5b403b510d0d0455468aeb98622b137dae857553ccd8883
a7bc37520e06e515d22c954eba5025b8cc57ee59418ce7dc6bc41556bdb36bbca3e87
74301fbcaa3b83b220809560987815f65286764703de0f3d524400a19b159610b11ef
3e
```

ciphertext #2:

```
234c02ecbbfbafa3ed18510abd11fa724fcda2018a1a8342cf064bbde548b12b07df4
4ba7191d9606ef4081ffde5ad46a5069d9f7f543bedb9c861bf29c7e205132eda9382
b0bc2c5c4b45f919cf3a9f1cb74151f6d551f4480c82b2cb24cc5b028aa76eb7b4ab2
4171ab3cdadb8356f
```

ciphertext #3:

```
32510ba9a7b2bba9b8005d43a304b5714cc0bb0c8a34884dd91304b8ad40b62b07df4
4ba6e9d8a2368e51d04e0e7b207b70b9b8261112bacb6c866a232dfe257527dc29398
f5f3251a0d47e503c66e935de81230b59b7afb5f41afa8d661cb
```

ciphertext #4:

```
32510ba9aab2a8a4fd06414fb517b5605cc0aa0dc91a8908c2064ba8ad5ea06a02905
6f47a8ad3306ef5021eafe1ac01a81197847a5c68a1b78769a37bc8f4575432c198cc
b4ef63590256e305cd3a9544ee4160ead45aef520489e7da7d835402bca670bda8eb7
75200b8dabbba246b130f040d8ec6447e2c767f3d30ed81ea2e4c1404e1315a1010e7
229be6636aaa
```

ciphertext #5:

```
3f561ba9adb4b6ebec54424ba317b564418fac0dd35f8c08d31a1fe9e24fe56808c21
3f17c81d9607cee021dafe1e001b21ade877a5e68bea88d61b93ac5ee0d562e8e9582
f5ef375f0a4ae20ed86e935de81230b59b73fb4302cd95d770c65b40aaa065f2a5e33
a5a0bb5dcaba43722130f042f8ec85b7c2070
```

ciphertext #6:

```
32510bfbacfbb9befd54415da243e1695ecabd58c519cd4bd2061bbde24eb76a19d84
aba34d8de287be84d07e7e9a30ee714979c7e1123a8bd9822a33ecaf512472e8e8f8d
b3f9635c1949e640c621854eba0d79eccf52ff111284b4cc61d11902aebc66f2b2e43
6434eacc0aba938220b084800c2ca4e693522643573b2c4ce35050b0cf774201f0fe5
2ac9f26d71b6cf61a711cc229f77ace7aa88a2f19983122b11be87a59c355d25f8e4
```

ciphertext #7:

```
32510bfbacfbb9befd54415da243e1695ecabd58c519cd4bd90f1fa6ea5ba47b01c90
9ba7696cf606ef40c04afe1ac0aa8148dd066592ded9f8774b529c7ea125d298e8883
f5e9305f4b44f915cb2bd05af51373fd9b4af511039fa2d96f83414aaaf261bda2e97
b170fb5cce2a53e675c154c0d9681596934777e2275b381ce2e40582afe67650b13e7
2287ff2270abcf73bb028932836fbdecfecee0a3b894473c1bbeb6b4913a536ce4f9b
13f1efff71ea313c8661dd9a4ce
```

ciphertext #8:

```
315c4eeaa8b5f8bffd11155ea506b56041c6a00c8a08854dd21a4bbde54ce56801d94
3ba708b8a3574f40c00fff9e00fa1439fd0654327a3bfc860b92f89ee04132ecb9298
f5fd2d5e4b45e40ecc3b9d59e9417df7c95bba410e9aa2ca24c5474da2f276baa3ac3
25918b2daada43d6712150441c2e04f6565517f317da9d3
```

ciphertext #9:

```
271946f9bbb2aeadec111841a81abc300ecaa01bd8069d5cc91005e9fe4aad6e04d51
3e96d99de2569bc5e50eeeca709b50a8a987f4264edb6896fb537d0a716132ddc938f
b0f836480e06ed0fcd6e9759f40462f9cf57f4564186a2c1778f1543efa270bda5e93
3421cbe88a4a52222190f471e9bd15f652b653b7071aec59a2705081ffe72651d08f8
22c9ed6d76e48b63ab15d0208573a7eef027
```

ciphertext #10:

```
466d06ece998b7a2fb1d464fed2ced7641ddaa3cc31c9941cf110abbf409ed3959800
5b3399ccfafb61d0315fca0a314be138a9f32503bedac8067f03adbf3575c3b8edc9b
a7f537530541ab0f9f3cd04ff50d66f1d559ba520e89a2cb2a83
```

target ciphertext (decrypt this one):

```
32510ba9babebbbefd001547a810e67149caee11d945cd7fc81a05e9f85aac650e905
2ba6a8cd8257bf14d13e6f0a803b54fde9e77472dbff89d71b57bddef121336cb85cc
b8f3315f4b52e301d16e9f52f904
```