

Cryptography: Assignment 3

Topics: Modes of Operation

1. Consider the CBC and CTR mode of operations and answer the following for each of these modes of operations.
 - (a) How do you encrypt a message of size 1050 bits assuming the underlying primitive is a 128-bit block cipher? What is the length of the resulting ciphertext?
 - (b) Suppose a single bit error has occurred in exactly two of the ciphertext blocks. Which plaintext blocks will it affect during the decryption?
2. Let F be a pseudorandom function mapping 128-bits to 128-bits. Consider the mode of operation using F where the encryption operation is performed as follows:
 - First, a uniform value $r \leftarrow_{\$} \{0, 1\}^{64}$ is chosen.
 - Then, for i -th plaintext block M_i , the i -th ciphertext block C_i is computed as
$$C_i := F_k(r \| i) \oplus M_i.$$
 - (a) What is the maximum message length that can be encrypted using this scheme?
 - (b) Does this scheme have indistinguishable encryptions in the presence of an eavesdropper?
3. Consider the following modes of operation, dubbed XEX (or Xor-Encrypt-Xor), that takes as input a message M of length ℓ blocks (a block consists of n bits) and returns a ciphertext C using a secure block cipher E described in Algorithm 1.

Algorithm 1 XEX Encryption

```
1: function XEX.ENC[E]( $K, M$ )
2:    $M_1 \| \dots \| M_\ell \leftarrow M$ 
3:    $R \leftarrow_{\$} \{0, 1\}^n$ 
4:   for  $i = 1$  to  $\ell$  do
5:      $C_i \leftarrow E_K(M_i \oplus R) \oplus R$ 
6:   end for
7:   return  $C = (R \| C_1 \| \dots \| C_\ell)$ 
8: end function
```

- (a) Write down the decryption procedure of XEX.
- (b) Comment on the following properties of XEX: (i) inverse-free, (ii) parallelism.
- (c) What is the effect of a single-bit error in the ciphertext?
- (d) Show that XEX does not achieve indistinguishability security under an eavesdropping adversary.

4. Let E be a pseudorandom permutation. Consider the mode of operation (variant of CTR mode) in which a uniform value $IV \leftarrow_{\$} \{0,1\}^n$ is chosen, and the i th ciphertext block C_i is computed as $C_i := E_k(IV + i + M_i)$, where addition operation is done modulo 2^n . The ciphertext is $C = (IV, (C_1, C_2, \dots))$. Show that this scheme is not Indistinguishable even under an EAV adversary.