COMS30023 / Cryptology

Problem Sheet 3

François Dupressoir *

2025/26

In this problem sheet, we exercise your mode of operations and reductions muscle. We'll look at different definitions of security—focusing mostly on the adversary's ability to fiddle with nonces—and see what we can see.

Most of the questions in this answer sheet are solid practice for standard exam questions. (1-star aiming for pass, 2-star aiming for 2:1, 3-star aiming for the stars.)

1. In the notes, we skip over defining a one-way notion for nonce-based encryption. However, the notion is useful to describe certain attacks (as we will do below). In this question, we will develop a suitable OW-CPA notion. For simplicity, we will assume that $\mathcal{M} = \{0,1\}^\ell$ for some $\ell > 0$.
   a) ⋆ Let's first concentrate on the adversary's goal, namely the "OW" part of OW-CPA security. Define a OW-PAS (one-wayness under passive attacks) security for nonce-based encryption schemes. Don't forget the nonce!
   b) ⋆ The next step is to add the adversary's power, namely the "CPA" part of OW-CPA security. Define a OW-CPA (one-wayness under chosen plaintext attack) security notion for nonce-based encryption schemes.

2. The idea of nonces is that they are unique. This question explores what happens when they are not.
   a) ⋆ Consider a (secure) blockcipher in counter mode and suppose an adversary sees two ciphertexts of the same length, both created using the same nonce, say $n = 0^{64}$. What can the adversary learn about the plaintexts?
   b) ⋆ Show that counter mode is not (even) OW–CPA if nonces can be repeated by the adversary.

3. Historically, many different modes other than CTR have been proposed. One of the most popular modes is cipher-block-chaining (CBC, see notes), which we'll look at in this question.
   a) ⋆ CBC mode is insecure when nonces are reused. Imagine an adversary trying to distinguish between the real and the ideal world by asking for encryptions of $(0^n, 0^n 1^n)$ and $(0^n, 0^n 0^n)$. Turn your observation into a chosen plaintext distinguishing attack. (Because it reuses a nonce, this is technically a nonce-misuse chosen plaintext attack.)
   b) ⋆⋆ In fact, CBC mode is not even secure when nonces are unique. Give a nonce respecting (no repeated nonces) chosen plaintext distinguishing attack with "reasonable" time and query complexity, and an advantage close to 1. Hint: two *adaptively* chosen messages suffice.

*Based on material by Dr. Martijn Stam, Dr David Bernhard and others

4. Given its insecurity, the popularity of CBC might at first be surprising. However, when the nonce is chosen *uniformly at random*, CBC is secure. In such a case the nonce is usually referred to as an *initialisation vector* (IV). An advantage of using a random value is that you do not need to worry about synchronizing across multiple devices; a disadvantage is that you rely on a good source of randomness (an expensive resource).

   a) $\star$ Imagine you use random values for the nonce and you encrypt q different messages. What is the probability that, by chance, you end up using the same nonce for two different messages?

   b) $\star\star$ Define "real" and "ideal" experiments to define an (IV)IND-CPA advantage for the random IV scenario. (In this setting, the adversary does not get to choose the nonce, but does get to see it.) It is easiest to first describe the real world and then ensure that the ideal world matches, so its oracle takes in the same kind of inputs, producing the same kind of outputs, and rejecting the same queries. Remember Kerckhoffs and nonces.

   c) $\star\star\star$ Nonce-based security implies IV-based security, as long as the probability the randomly chosen IVs collide can be contained. A semi-formal statement is that for any nonce-based encryption scheme Enc and any adversary $\mathbb{A}_{(\mathsf{iv})\mathsf{ind}}$ making q queries, there exists an equally efficient adversary $\mathbb{B}_{(\mathsf{n})\mathsf{ind}}$ such that

$$\mathsf{Adv}^{(\mathsf{iv})\mathsf{ind}}_{\mathsf{Enc}}(\mathbb{A}_{(\mathsf{iv})\mathsf{ind}}) \leq \mathsf{Adv}^{(\mathsf{n})\mathsf{ind}}_{\mathsf{Enc}}(\mathbb{B}_{(\mathsf{n})\mathsf{ind}}) + q^2/\,|\mathcal{N}|$$

   Define a reduction that proves this statement, and analyse it.

   The consequence of the birthday bound $q^2/\,|\mathcal{N}|$ in the statement above, coupled with a desire to allow nonce-based schemes to be used with randomly chosen IVs, is that the nonce space must be large. To give a concrete benchmark, a recent lightweight competition required that $|\mathcal{N}| \geq 2^{96}$. The low end of that range is only acceptable because the lightweight standards make serious recommendations about re-keying.

5. CFB and OFB are two other modes of operation. CFB stands for cipher feedback mode. OFB stands for output feedback mode. For both, the encryption routines are depicted below, CFB to the left and OFB to the right (where we've omitted the parsing and recombining of messages and ciphertexts into blocks and back).

$\mathsf{CFB.Enc}(\mathsf{E})^n_k(m[1], \ldots, m[n])$
$c[0] \leftarrow n$
for $i \in [1, \ldots, n]$
$\quad X[i] \leftarrow \mathsf{E}_k(c[i-1])$
$\quad c[i] \leftarrow m[i] \oplus X[i]$
return $c[1], \ldots, c[n]$

$\mathsf{OFB.Enc}(\mathsf{E})^n_k(m[1], \ldots, m[n])$
$X[0] \leftarrow n$
for $i \in [1, \ldots, n]$
$\quad X[i] \leftarrow \mathsf{E}_k(X[i-1])$
$\quad c[i] \leftarrow m[i] \oplus X[i]$
return $c[1], \ldots, c[n]$

   For each of the two modes:

   a) $\star$ Define the decryption algorithms.

   b) $\star$ If you had to compare with the other two modes we have seen so far (CBC, CTR), which mode do you find most similar?

   c) $\star\star$ Comment on the efficiency. Are encryption or decryption parallelizable? Does decryption require the decipher functionality of the blockcipher?

   d) $\star\star\star$ Comment on the mode's security.