(1.) a.) OW-PAS

Let $\mathcal{E}$ be a nonce-based encryption scheme. We define the advantage of $\mathcal{A}$ in passively breaking one-wayness as follows:

$$\mathrm{Adv}^{(n)\text{ow-pas}}_{\mathcal{E}}(\mathcal{A})$$

$$= \Pr\left[\mathrm{Exp}^{(n)\text{ow-pas}}_{\mathcal{E}}(\mathcal{A}) : \hat{m} = m^*\right]$$

where $\mathrm{Exp}^{(n)\text{ow-pas}}_{\mathcal{E}}(\mathcal{A})$ is:

$k \xleftarrow{\$} \mathcal{K}g$

$n \xleftarrow{\$} \mathbb{N}$

$m^* \xleftarrow{\$} \mathcal{M}$

$c^* \leftarrow E^n_k(m^*)$

$\hat{m} \xleftarrow{\$} \mathcal{A}(c^*)$

$m \xleftarrow{\$} A(c^*)$ ✓

Very Good!

b.) OW-CPA

$Adv^{(n)ow\text{-}cpa}_{E_1}(A)$

$= Pr\left[Exp^{(n)ow\text{-}cpa}_{E_1}(A) : \hat{m} = m^*\right]$ ✓

where $Exp^{(n)ow\text{-}cpa}_{E_1}$ is:

$k \xleftarrow{\$} kg$ ✓

$m \xleftarrow{\$} M$ ✓

$m^* \xleftarrow{\$} \mathcal{M}$ ✓

$\hat{m} \leftarrow A^{\mathcal{E}(\cdot,\cdot)}$ ✓

and $\mathcal{E}(n, m)$

no repeat nonces

$c \leftarrow \tilde{E}^n_{k^*}(m)$ ✓

return c ✓

Very Good

2. a) Each part of both ciphertexts is generated as

$$C_i = m_i \oplus Y_i$$

Y_i is identical between both ciphertexts, so this is identical to the situation of knowing the key in OTP (without actually knowing the key in this case)

$$C_1 \oplus C_2 = (m_1 \oplus Y) \oplus (m_2 \oplus Y)$$

$$\downarrow \text{ as } Y \oplus Y = 0$$

✓ Good

$$C_1 \oplus C_2 = m_1 \oplus m_2$$

∴ the adversary can learn the result of XOR'ing the two

plaintexts Goal: recover plaintext

b) If nonces can be repeated, the adversary can get the original plaintext, by XOR'ing C^* with a C generated with the same nonce, and then XOR'ing this with the chosen plaintext used to produce C, thus breaking one-wayness

(3) a) The first block (length n)

of ciphertext for both encryptions will be identical, The next blocks should differ.

If this is the case it should be the real world.

✓

Maybe some calculations would be appreciated

b) In CBC,

$$C[1] = E_k(m[1] \oplus n)$$

If $n_1 = 0^n$ and $m_1 = 0^n$

then $C_1 = E_k(0^n)$

✓

If $n_2 = 1^n$ and $m_2 = 1^n$

then $c_2 = E_k(0^n)$

If $c_1 = c_2$ then it should be real.

(4.) a.) Same principle as the birthday bound:

$$\frac{q \cdot (q-1)}{2 \cdot |N|}$$

Good

when N is the set of all

nonces.

b.)

$\text{Exp}_{E}^{(\text{IV})\text{ind-cpa-real}}(A)$

$k^* \xleftarrow{\$} Kg$

$IV \xleftarrow{\$} \mathcal{N}$

$b \xleftarrow{\$} A^{\mathcal{E}(IV,\cdot)}$

where $\mathcal{E}(IV, m)$ is:

no repeat nonces

$C \leftarrow \text{Enc}_{k^*}^{IV}(m)$

return C, n

$\text{Exp}_{E}^{(\text{IV})\text{ind-cpa-ideal}}(A)$

$IV \xleftarrow{\$} \mathcal{N}$

$b \xleftarrow{\$} A^{\mathcal{E}(IV,\cdot)}$

where $\mathcal{E}(IV, m)$ is:

no repeat nonces

$C \xleftarrow{\$} C(|m|)$

return C, n

$\text{Adv}_{E}^{(\text{IV})\text{ind-cpa}}(A)$

$$Adv_{E}^{(iv)\,ind\text{-}cpa}(A) = Pr\left[Exp_{E}^{(iv)\,ind\text{-}cpa\text{-}real}(A) : \hat{b} = 1\right]$$

$$- Pr\left[Exp_{E}^{(iv)\,ind\text{-}cpa\text{-}ideal}(A) : \hat{b} = 1\right]$$

c.) May eventually come back to this

Or

5 a.)

$$CFB.Dec(E)_{K}^{n}(C[1], \ldots C[n])$$

$C[0] \leftarrow n$

for $i \in [1, \ldots n]$:

$X[i] \leftarrow E_{k}(C[i-1])$

$m[i] \leftarrow C[i] \oplus X[i]$

return $m[1], \ldots, m[n]$

OFB. $Dec(t)^{n}_{k}(c[1], \ldots c[n])$

$X[0] \leftarrow n$

For $i \in [1, \ldots, n]$:

$X[i] \leftarrow E_k(X[i-1])$ ✓

$m[i] \leftarrow c[i] \oplus X[i]$

return $m[1], \ldots, m[n]$

b.) CBC is more similar as both are dependent on previous parts of the blockciphe ✓

ut

c.) As stated in b.), not parallelizable.

You mean a unique decryption function?

It does not actually require the decryption, which could be efficient in terms of memory (less space required to store algorithm) and speed (less storage - higher priority cache)

Sure

d.) Succeptible to plaintext distinguishing when nonces are re-used. Same distinguishing method can be used by

adaptively choosing 2 messages

Good!