CA

Problem Sheet 3 (1)

1) (a) $\text{Exp}^{(n)\text{ow-cpa}}_{E}(A)$

$k \xleftarrow{\$} \{0,1\}^n$ — we also need to declare some nonce n

$n \xleftarrow{\$} \mathcal{N}$

$m \leftarrow A$

$c \leftarrow \mathcal{E}_k(m, n)$ ✓

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

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

no repeat nonce, can't use real nonce

$c \leftarrow \mathcal{E}(n, m)$ ✓

return c

2) a) The adversary can learn if the messages are the same or not (true) and learn the message! → they can learn together the plaintext

b) encrypt 0 with the same nonce

using the notation from the below notes we get

$c_0[i] = m_0[i] \oplus Y[i]$

$c_1[i] = m_1[i] \oplus Y[i]$

$c_1[i] \oplus c_0[i] = m_0[i] \oplus Y[i] \oplus Y[i] \oplus m_1[i]$

$= m_0[i] \oplus m_1[i]$

∞ if $m_1[i] = 0 \Rightarrow c_0[i] \oplus c_1[i] = m_0[i]$ ✓ lovely!

and we can recover the message

3) a) $(0^n, 0^n 0^n)$

$(0^n, 0^n 1^n)$

In the real world the first half of the ciphertext will be the same, while in the ideal world there will be 2 random ciphertexts.

⇒ the adversary can distinguish between the 2 worlds ✓

b) m_0 is picked at random

$m_0[1] \ldots [x]$

‖ encrypted with nonce n_0 under k

$c_0[0]$ $[1]$ ‖ ‖ and so on

n_0 $E_k(m_0[1] \oplus n_0)$

↳ choose this as n_1

and $m_1 = m_0[2][3] \ldots$

$\Rightarrow$

$c_1[0]$ $c_1[1]$ $[2]$

$E_k(m_0[1] \oplus n_0)$ $E_k(m_1[2] \oplus E(m_0[1] \oplus n_0))$

$c_0[2]$

$\Rightarrow$ we can distinguish between the 2 worlds

yes! Very nice.

4) a) $\frac{q(q-1)}{2|N|}$ ✓ using the same explanation that was given in the lectures

$\frac{q^2}{|N|} \leq$

b)

(IV) IND-REAC (A)

$k \xleftarrow{\$} K_E$

$n \xleftarrow{\$} N$

$\hat{b} \leftarrow A^{\mathcal{E}(\cdot)}$

no repeat nonces

$\mathcal{E}(m)$

$n' \xleftarrow{\$} N$

$c \leftarrow \text{Enc}_k(m; n')$

return c, n

(IV) IND-IDEAL (A)

$k \xleftarrow{\$} K_E$

$n \xleftarrow{\$} N$

$\hat{b} \leftarrow A^{\mathcal{E}(\cdot)}$

no repeat nonces

$\mathcal{E}(m)$

$c \xleftarrow{\$} \mathcal{C}$

return c, n

$n \xleftarrow{\$} N$ is in the oracles as A doesn't control it

c) this is just a statement, not a question ← good point.

Effectively, show the reduction i.e. construct the adversary $\mathcal{B}$ with A as a black box.

5)

a) CFB

```
c[0] = n
for i ∈ {1,...,n}
    y[i] = Enc(c[i-1])
    m[i] = c[i] ⊕ y[i]
return m
```

OFB

```
X[0] = n
for i ∈ {1,...,n}
    X[i] = ξ_k(X[i-1])
    m[i] = c[i] ⊕ X[i]
return m
```

b) They are similar to CBC

c) Both encryption and decryption can't be parallelized as you need the previous result to calculate the current one inside the for loop.

I'm not sure what is meant by the decipher functionality of the blockcipher.

deciphering functionality means that a separate $Dec_k(\dots)$ is need on top of $Enc_k(\dots)$. This is specific to the primitives of the block cipher and not the block cipher itself

d) Both are secure under a 1 time attack as there is no way to distinguish between the real world and the ideal world

Similarly to CBC, if nonces can repeat, the scheme is not secure.

If nonces can't repeat, using the same strategy used for CBC we can distinguish between the 2 worlds.