

CA

# Problem Sheet 3

1) (a)

(n) OW-CPA

Exp

(A)

$k \xleftarrow{\$} K$   
 $n \xleftarrow{\$} N$   
 $m \xleftarrow{\$} M$

we also need to declare some nonce  $n$

$c \leftarrow E_k(m, n)$

$\hat{m} \leftarrow A(c, \dots)$

(b)  $E(n, m)$

no repeat nonce, can't use real nonce

$c \leftarrow E(n, m)$

return  $c$

2) a) The adversary can learn if the messages are the same or not and learn the message!  $\rightarrow$  they can learn the plaintext

b) encrypt 0 with the same nonce using the notation from the below notes we get

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

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

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

if  $m_1[i] = 0 \Rightarrow c_0[i] \oplus c_1[i] = m_0[i]$  and we can recover the message lovely!

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.

$\Rightarrow$  the adversary can distinguish between the 2 worlds

b)  $m_0$  is picked at random

$m_0[1] \dots [x]$   
|| encrypted with nonce  $n_0$  under  $k$

$$c_0[0] \quad [1] \quad \dots$$

$$n_0 \quad \left( E_k(m_0[1] \oplus n_0) \right)$$

and so on

$\hookrightarrow$  choose this as  $m_1$

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

(2)

$\Rightarrow$

$$\begin{array}{ccc} C_1[0] & C_1[1] & L[0] \\ \downarrow & \downarrow & \\ E_k(m_0) \oplus u_0 & E_k(m_1) \oplus E(m_0) \oplus u_0 \end{array}$$

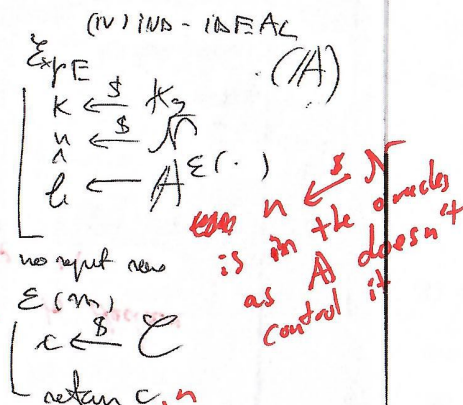
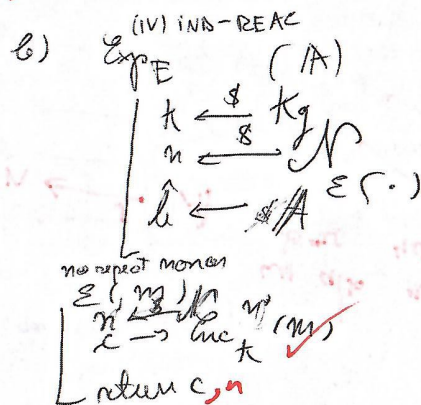
$C_0[2]$

yes! Very nice.

we can distinguish between the 2 worlds

4) a)  $\frac{2^2}{|N|} \leq \frac{2(g-1)}{2|N|}$

using the same explanation that was given in the lecture



is in the oracle as A doesn't control it

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

Effectively, show the reduction i.e. make construct the adversary B with A as a black box.



5) CFB

a)  $\Delta$   
 $c[0] = n$   
 for  $i \in \{1 \dots n\}$   
 $y[i] = \text{Enc}(c[i-1])$   
 $m[i] = d[i] \oplus y[i]$   
 return  $m$

OFB

$\Delta$   
 $x[0] = n$   
 for  $i \in \{1 \dots n\}$   
 $x[i] = E_k(x[i-1])$   
 $m[i] = c[i] \oplus x[i]$   
 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  $\text{Dec}_k(\cdot)$  is needed on top of  $\text{Enc}_k(\cdot)$ . This is specific to the internals 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.