1 - Flavours of IND-CCA

Question 1 :

To show that IND-CCA-1 security implies IND-CCA-2 security we define :

The advantage of IND-CCA-1 is negligeable and for all ppt adversaries $\mathcal{A}$, the advantage is :

$$Adv^{ind-cca-2}_{\mathcal{A}, PKE} = 2 \Pr[\text{IND-CCA-2}_{PKE}(\mathcal{A}) \Rightarrow true] - 1$$

$$= 2 \Pr[b == b' \wedge ct^* \notin \mathcal{L}_1 \wedge ct^* \notin \mathcal{L}_2] - 1$$

$$\leq 2 \Pr[b == b' \wedge ct^* \notin \mathcal{L}_2] - 1$$

$$\leq 2 \Pr[b == b' \wedge ct^* \notin \mathcal{L}_2] - 1$$

$$\leq 2 \Pr[\text{IND-CCA-1}_{PKE}(\mathcal{A}) \Rightarrow true] - 1$$

$$\leq Adv^{ind-cca-1}_{\mathcal{A}, PKE}$$

Knowing that the Advantage of IND-CCA-1 is negligeable so is the one of IND-CCA-2 which prove that IND-CCA-1 security $\Rightarrow$ IND-CCA-1 security

Question 2

To Prove IND-CCA-3 security implies IND-CCA-1 security we define :

The advantage of IND-CCA-3 is negligeable and for all adversaries ppt $\mathcal{A}$, we have an adversary that never queries ODec2(ct^*), the advantage is :

which one ? define it

- 0.5pt

$$Adv^{ind-cca-1}_{\mathcal{A}, PKE} = 2 \Pr[\text{IND-CCA-1}_{PKE}(\mathcal{A}) \Rightarrow true] - 1$$

$$= 2 \Pr[b == b' \wedge ct^* \notin \mathcal{L}_2] - 1$$

$$= 2 \Pr[ct^* \notin \mathcal{L}_2] \cdot \Pr[b == b' \mid ct^* \notin \mathcal{L}_2] - 1$$

Here we have $\Pr[ct^* \notin \mathcal{L}_2] = 1$ because we never query the oracle that fill $\mathcal{L}_2$ and we have that $b == b'$ is independent from $ct^* \notin \mathcal{L}_2$ since the choice of b' doesn't depend on ODec2(ct) so we have :

not sure ...

$$= 2 \Pr[b == b'] - 1 = Adv^{ind-cca-3}_{\mathcal{A}, PKE}$$

Knowing that the advantage of IND-CCA-3 is negligeable we proved that the advantage of IND-CCA-1 is also negligeable which mean that IND-CCA-3 security implies IND-CCA-1 security

Question 3

We have to show that a well-spread IND-CCA-2 secure PKE is also IND-CCA-1 secure, that we define : The advantage of IND-CCA-2 to be negligeable and for all ppt $\mathcal{A}$ we have :

$$
\begin{aligned}
\mathrm{Adv}^{ind-cca-1}_{\mathcal{A},PKE} &= 2\Pr[\text{IND-CCA-1}_{PKE}(\mathcal{A}) \Rightarrow \text{true}] - 1 \\
&= 2\Pr[b == b' \wedge ct^* \notin \mathcal{L}_2] - 1 \\
&= 2\Pr[b == b' \wedge ct^* \notin \mathcal{L}_1 \wedge ct^* \notin \mathcal{L}_2] - 1 + 2\Pr[b == b' \wedge ct^* \in \mathcal{L}_1 \wedge ct^* \notin \mathcal{L}_2] \\
&= 2\Pr[\text{IND-CCA-2}_{PKE}(\mathcal{A}) \Rightarrow \text{true}] - 1 + 2\Pr[b == b' \wedge ct^* \in \mathcal{L}_1 \wedge ct^* \notin \mathcal{L}_2] \\
&\leqslant \mathrm{Adv}^{ind-cca-2}_{\mathcal{A},PKE} + 2\Pr[ct^* \in \mathcal{L}_1]
\end{aligned}
$$

no. $\mathbb{P}(ct^* \in L_1) \leqslant \mathbb{P}\Big(\bigcup_{ct \in L_1} ct^* = ct\Big) \leqslant q\gamma$

$$
\begin{aligned}
&\leqslant \mathrm{Adv}^{ind-cca-2}_{\mathcal{A},PKE} + \max_{ct^* \in \mathcal{L}_1} 2\Pr[ct^* = \mathrm{Enc}(pk, pt)] \\
&\leqslant \mathrm{Adv}^{ind-cca-2}_{\mathcal{A},PKE} + \max_{ct^* \in \mathcal{C}} 2\Pr[ct^* = \mathrm{Enc}(pk, pt)] \\
&\leqslant \mathrm{Adv}^{ind-cca-2}_{\mathcal{A},PKE} + 2\gamma
\end{aligned}
$$

$-0.5pt$

Knowing that the advantage of IND-CCA-2 is negligeable and that it is well-spread the γ is a negligeable value so twice a negligeable value is a negligeable value and the sum of negligeable value is a negligeable value. So the advantage of IND-CCA-1 is negligeable which mean that A well-spread IND-CCA-2 secure PKE $\Rightarrow$ IND-CCA-1 secure

Question 4

If an adversary can find ct' such that $\Pr[\mathrm{Enc}(pk, \mathrm{Dec}(sk, ct')) = ct'] = 1$, he just has to query it to ODec 1 and return $pt_1 = \mathrm{Dec}(sk, ct')$, pt_2, ct' where pt_2 is a random plaintext.

In the second phase, $\mathcal{A}$ compares ct^* with ct'. If they are equals it returns pt_1, if not it returns pt_2. And with the IND-CCA-1 game with an advantage Adv mean 1. But it loses the IND-CCA-2 game with an advantage Adv mean 0, because of ODec (ct'). So the well-spreadness is needed.

2 - A PKE in QR_{m^2}

Question 1 :

If factoring is easy, one can easily compute $\lambda(m)$ and then :

$$h = g^{x} \pmod{m^2}$$
$$\Rightarrow h^{\lambda(m)} = (g^{x})^{\lambda(m)} \pmod{m^2}$$
$$\Rightarrow h^{\lambda(m)} = (g^{\lambda(m)})^{x} \pmod{m^2}$$
$$\Rightarrow h^{\lambda(m)} = (1+m)^{x} \pmod{m^2}$$
$$\Rightarrow h^{\lambda(m)} = \sum_{k=0}^{x} \binom{x}{k} m^{k} \pmod{m^2}$$

- We used the formula given in the exercise that $g^{\lambda(m)} = 1 + m \pmod{m^2}$
- We use the Binomial theorem where $(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{(m-k)} b^{k}$.

And we use the fact that for $k \geq 2$, $m^k = 0 \pmod{m^2}$

$$\Rightarrow h^{\lambda(m)} = 1 + xm \pmod{m^2}$$
$$\Rightarrow h^{\lambda(m)} - 1 = xm \pmod{m^2}$$

Knowing that $x < m \Rightarrow xm < m^2$. Meaning we have $x = \dfrac{(h^{\lambda(m)} - 1 \pmod{m^2})}{m}$

If we can compute x we can solve the discrete logarithm modulo m problem.

Question 2

For the decryption algorithm we have the cyphertext $ct = (U, V)$ and the secret key a.
To get the plaintext back we have to compute :

$$U^{-a} . V \bmod m^2 = 1 + mm$$
$$\Rightarrow U^{-a} . V - 1 \bmod m^2 = mm$$

And knowing that $m < m$ we have $mm < m$. So $m = \dfrac{(U^{-a} . V - 1 \bmod m^2)}{m}$

The operations to get back m are all deterministics meaning the decryption algorithm is deterministic so the result will always be the plaintext m as long as we have the good secret key and genuine cyphertexts.

Question 3

A security game capturing the one-wayness property of QRPKE can be:

Game :

1: $(g, m) \xleftarrow{\$} \mathrm{ParGen}(1^{\lambda})$
2: $a \xleftarrow{\$} \{1, ..., QR_{m^2}\}$
3: $h \leftarrow g^{a} \bmod m^2$
4: $pt \xleftarrow{\$} \mathbb{Z}_m$
5: $(U, V) \leftarrow \mathrm{Enc}((g, h, m), pt)$
6: $pt' \leftarrow \mathcal{A}(g, h, m, U, V)$
7: return $1_{pt == pt'}$

The advantage Adv must be negligible in λ and $Adv = \Pr[\mathrm{QRPKE}(\mathcal{A}) \Rightarrow \mathrm{true}]$

Question 4

If we can factor n, one can compute the discrete logarithm as proved in question 1 of $h = g^a$ and recover the secret key. Then with the knowledge of the secret key, one can decrypt easily anything and break the one-wayness of QRPKE. no, you'll get a mod n not a mod |G| -2pt

Question 5

We have to prove that the QR Diffie-Hellman problem is hard, QRPKE is one way.
To prove that we define an Adversary $\mathcal{B}$ that play the one-wayness game define in question 3.
We build an adversary $\mathcal{A}$:

you should prove Z mod n is a valid ciphertext with the correct distribution
-1pt

$\mathcal{A}(n, g, X, Y, Z \bmod n)$:
$\quad m \longleftarrow \mathcal{B}(g, X, n, Y, Z \bmod n)$
$\quad res \longleftarrow (Z \bmod n)(1 + mn)^{-1} \bmod n^2$
$\quad$ return res

Here $1 + mn = g^{m\lambda(n)} \bmod n^2$ has saw in previous question and it is also a proof that it is invertible.

So if $\mathcal{B}$ wins, $\mathcal{A}$ wins as well.
If QRPKE isn't one-way then QR Diffie-Hellman is not hard by contradiction we have
If QR Diffie-Hellman is hard then QRPKE is one-way.