1. **[11 marks] Short answer.**

   (a) **[4 marks]** For each of the following statements, circle **TRUE** if the statement is True or **FALSE** if the statement is False. *No explanation required.*

$110n^2 + 111 \in \Theta(n^2)$	[✓ TRUE]	FALSE
$\log_{110}(n) \in \Theta(\log_{111}(n))$	[✓ TRUE]	FALSE
$110^n + n^{111} \in \Theta(111^n + n^{110})$	TRUE	[✓ FALSE]
$\frac{1}{n+1} \in \Theta(1)$	[✓ TRUE]	FALSE
$\forall f, g : \mathbb{N} \to \mathbb{R}^{\geq 0},\ g \in \Theta(f) \Rightarrow g \in \Omega(f)$	[✓ TRUE]	FALSE
$\forall f, g : \mathbb{N} \to \mathbb{R}^{\geq 0},\ g \in \mathcal{O}(f) \Rightarrow f + g \in \Theta(f)$	[✓ TRUE]	FALSE
$\forall f, g : \mathbb{N} \to \mathbb{R}^{\geq 0},\ g \in \Omega(f) \Rightarrow f + g \in \Theta(f)$	TRUE	[✓ FALSE]
$\forall f, g : \mathbb{N} \to \mathbb{R}^{\geq 0},\ g \in \mathcal{O}(f) \Rightarrow (\forall n \in \mathbb{N},\ g(n) \leq f(n))$	TRUE	[✓ FALSE]

(b) **[2 marks]** Two people, *Alice* and *Bob*, want to communicate securely with a **public-key cryptosystem**. Alice generates a key pair with public key $pubKey_A$ and private key $priKey_A$. Bob generates a key pair with public key $pubKey_B$ and private key $priKey_B$.

In the table below, write down which of the four keys ($pubKey_A$, $priKey_A$, $pubKey_B$, $priKey_B$) is used for each action. *No explanation required.*

Action	**Key Used**
Alice encrypts a plaintext message to send to Bob	$pubKey_B$
Alice decrypts a ciphertext message from Bob	$priKey_A$
Bob encrypts a plaintext message to send to Alice	$pubKey_A$
Bob decrypts a ciphertext message from Alice	$priKey_B$

(c) **[1 mark]** Recall our implementation of the RSA cryptosystem from lecture. One of its limitations was that it encrypted the plaintext message *one character at a time* to produce the ciphertext.

Explain why this is considered not secure in practice (even when the modulus n is large). You may use an example ciphertext like `'OLaTO+T^+NZZW'` in your response.

One of the main drawbacks is that identical characters are encrypted to the
same character. Since the length and order of characters is maintained
in RSA cryptography, this can help the eavesdropper predict the
ciphertext. For example: 'OLaTO+T^ +NZZW' might be encrypted
to 'SapRS-R+-VBBT', as an eavesdropper I can see that the
first and fourth character is same, the two penultimate characters are
repeated too! If the message was a legible one, the eavesdropper could have guessed it