

Name+Surname: \_\_\_\_\_

Univ. Code: \_\_\_\_\_

**Q1:** For these questions, no need to provide derivation, just provide final result + brief explanation if/when necessary/requested

<b>Let <math>G</math> and <math>G_t</math> be groups with generators <math>g</math> and <math>g_t</math> respectively, assume a Bilinear Pairing <math>e(G,G) \rightarrow G_t</math> and either</b> <ul style="list-style-type: none"> <li>• simplify the following expression</li> <li>• or state why the expression is meaningless</li> </ul>	$e(a \times g^b, g^c) \rightarrow$	
	$e(g^a + g^b, g^c) \rightarrow$	
	$e(g^{a+b}, g^c) \rightarrow$	
<b>Consider group <math>Z_{8039}^*</math> - without performing any computation, state whether each of the following results mod 8039: (NB: 4019 is a prime number)</b> <ul style="list-style-type: none"> <li>• Is surely <b>correct</b>, no comp. needed</li> <li>• Is surely <b>wrong</b>, no comp. needed</li> <li>• We should <b>check</b> via computation</li> </ul> <p>In the answer, <b>briefly explain why</b></p>	$8038^{3455} = 5574$	
	$81^{4019} = 1$	
	$1301^{4019} = 1$	
	$13^{12057} = 7542$	

**Q2:** Multiple answer questions (comments can be added on the right if/when necessary)

The Pedersen Commitment $C(x,r) = g^x h^r \text{ mod } p$ is:	<ol style="list-style-type: none"> <li>1. Computationally hiding and comp. binding</li> <li>2. Computationally hiding and perfectly binding</li> <li>3. Perfectly hiding and comp. binding</li> <li>4. Perfectly hiding and perfectly binding</li> </ol>
A $(t,n)$ secret sharing scheme is ideal if	<ol style="list-style-type: none"> <li>1. The size of a share is equal to <math>1/t \times \text{size of the secret}</math></li> <li>2. The size of a share is equal to <math>1/n \times \text{size of the secret}</math></li> <li>3. The size of a share is equal to the size of the secret</li> <li>4. The size of a share is equal to <math>t \times \text{size of the secret}</math></li> <li>5. The size of a share is equal to <math>n \times \text{size of the secret}</math></li> </ol>
Consider an El Gamal Encryption scheme based on a prime modulus of 2048 bits. Assume you encrypt a message of 1024 bits. The size of the ciphertext (all included) is...	<ol style="list-style-type: none"> <li>1. 1024 bit</li> <li>2. 1024 bit + the size of the chosen IV</li> <li>3. 2048 bit</li> <li>4. 2048 bit + the size of the chosen IV</li> <li>5. 3072 bit</li> <li>6. 4096 bit</li> </ol>
The group order for an Elliptic Curve built over $\mathbb{Z}_p$ is	<ol style="list-style-type: none"> <li>1. Always equal to <math>p</math></li> <li>2. Always lower than <math>p</math></li> <li>3. Always larger than <math>p</math></li> <li>4. Can be lower or larger than <math>p</math></li> </ol>
Consider a Joux 3-way Diffie-Hellman construction based on a pairing $e(G,G) \rightarrow G_t$ – being $P_x$ the public coefficient exchanged by party $x$ , and $S$ the resulting shared secret:	<ol style="list-style-type: none"> <li>1. <math>P_x</math> and <math>S</math> are both points of group <math>G</math></li> <li>2. <math>P_x</math> and <math>S</math> are both points of group <math>G_t</math></li> <li>3. <math>P_x</math> is a point of group <math>G</math>, while <math>S</math> is a point of group <math>G_t</math></li> <li>4. <math>P_x</math> is a point of group <math>G_t</math>, while <math>S</math> is a point of group <math>G</math></li> </ol>

**Q3:** Find all the points of the EC group defined by equation  $y^2=x^3+5$  over  $\mathbb{Z}_7$

**Q4** Show how the private key can be computed if the nonce is reused in an ECDSA signature

Name+Surname: \_\_\_\_\_ Univ. Code: \_\_\_\_\_

**Q5 Assume arithmetic modulus 101.** A Linear secret sharing scheme involving 4 parties is described by the following access control matrix:

A:	1	1	0
B:	1	0	1
C:	0	1	1
D:	0	0	1

**A.** Compute the secret assuming that shares B → 22, D → 9 are revealed

**B.** Compute the secret assuming that shares A → 45, B → 22, C → 41 are revealed (for this case show step by step how you arrived to the result)

**Q6** Describe the Boneh-Franklin Identity Based Encryption scheme