

Network Security – prof. Giuseppe Bianchi – 3rd term exam, 5 February 2024

Name+Surname: _____ Univ. Code: _____

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

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

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"> 1. Computationally hiding and comp. binding 2. Computationally hiding and perfectly binding 3. Perfectly hiding and comp. binding 4. Perfectly hiding and perfectly binding
A (t, n) secret sharing scheme is ideal if	<ol style="list-style-type: none"> 1. The size of a share is equal to $1/t \times$ size of the secret 2. The size of a share is equal to $1/n \times$ size of the secret 3. The size of a share is equal to the size of the secret 4. The size of a share is equal to $t \times$ size of the secret 5. The size of a share is equal to $n \times$ size of the secret
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"> 1. 1024 bit 2. 1024 bit + the size of the chosen IV 3. 2048 bit 4. 2048 bit + the size of the chosen IV 5. 3072 bit 6. 4096 bit
The group order for an Elliptic Curve built over Z_p is	<ol style="list-style-type: none"> 1. Always equal to p 2. Always lower than p 3. Always larger than p 4. Can be lower or larger than p
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"> 1. P_x and S are both points of group G 2. P_x and S are both points of group G_t 3. P_x is a point of group G, while S is a point of group G_t 4. P_x is a point of group G_t, while S is a point of group G

Q3: Find **all** the points of the EC group defined by equation $y^2 = x^3 + 5$ over 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 $B \rightarrow 22$, $D \rightarrow 9$ are revealed

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

Q6 Describe the Boneh-Franklin Identity Based Encryption scheme