Departamento de Mate	emática	Faculdade de Ciência	as e Tecnologia — UNL
Criptografia	05	/06/2019	Teste
	Duração do '	TESTE: 1 HORA	
0 0 0 0 0	drados respectivos d	a grelha ao lado (🔳) e e	ndo completamente os qua- screva o nome completo, o
	número e o curso aba	aixo.	
2 2 2 2 2 3 3 3 3 3	Nome:		
4 4 4 4 4			
5 5 5 5 5 6 6 6 6 6	Número:	Curso:	
7 7 7 7 7 8 8 8 8 8 9 9 9 9 9 9	resposta certa preenc	hendo completamente o qu	a resposta certa. Marque a adrado respectivo () com 0,5 valores. Cada resposta
	errada desconta 0,2 v Das questões 7, 8 e	valores. Marcações múltipl	as anulam a questão. ema diferente do seminário

\mathbf{Q}	uestão	1	. As o	luas	técnicas	base	da	cript	tograf	ia c	le i	chave	simétrica	a são
--------------	--------	---	--------	------	----------	------	----	-------	--------	------	------	-------	-----------	-------

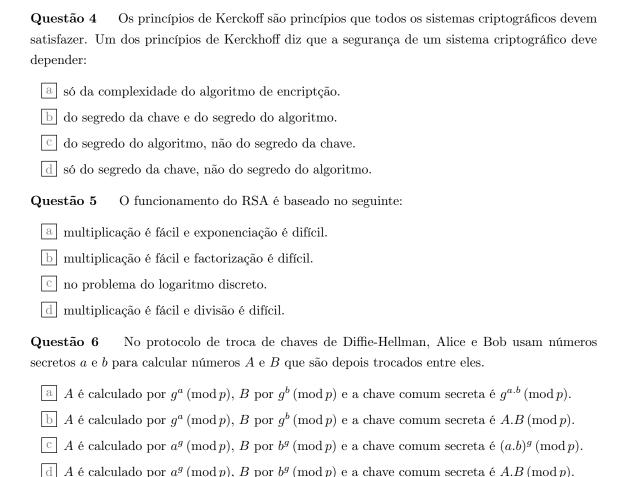
a transposição e permutação. c permutação e substituição. b transposição e substituição. d nenhuma das restantes opções.

O ADFGVX Questão 2

- a é um protocolo de chave simétrica, que usa as duas técnicas base.
- b é um protocolo de chave assimétrica, não vulnerável ao man-in-the-middle.
- © é um protocolo de chave simétrica, que usa apenas uma das técnicas base.
- d é um protocolo de chave assimétrica, vulnerável ao man-in-the-middle.

Questão 3 Qual das seguintes afirmações é FALSA. Ao codificar uma mensagem a máquina Enigma

- a pode codificar a mesma letra por letras diferentes.
- pode codificar uma letra por ela própria.
- nenhuma das restantes opções.
- d pode codificar letras diferentes pela mesma letra.



Questão 7

Descreva detalhadamente o DES, explicando pontos fortes e vulnerabilidades.

Questão 8

Enuncie e demonstre o teorema de Euler.

Questão 9

Explique o que é uma assinatura digital e explique detalhadamente o uso do RSA para assinaturas digitais.