



## Försättsblad tentamen / Examination cover

And	nym	itets	kod	/ An	onyr	nous	s cc	ode															
S	-	0	0	5	-	0	9																
Kur	skod	/ Co	ourse	e co	de			Prov	/kod	/Te	st co	de		Ten	tame	ensd	atun	n/E	xam	inati	on d	ate	
D	Т	0	2	4	Α			Q	1	0	2			2	0	1	8	-	0	2	-	1	5
Kur	snar	nn /	Cou	rse r	name	Э							- "										
Da	Datateknik AV, Nätverkssäkerhet och nätverksdrift																						
Pro	Provnamn / Test name																						
Αι	Automaträttat (flervals) prov																						

## Skriv din anonymitetskod på varje inlämnat papper Write your anonymous code on each sheet submitted

## Sätt ett kryss (x) för varje inlämnad uppgift

Use an x to indicate which questions has been submitted

Markera Mark belo	nedan med X / ow with an X	Credit	Lärarens anteckningar / Teacher's notes	Markera r Mark belo	edan med X / w with an X	Poäng / Credit	Lärarens anteckningar / Teacher's notes
1	X	19		16			
2	X	19		17			
3	X	15		18			
4	X	20		19			
5	X	20		20			
6				21			
7				22			
8				23			
9				24			
10				25			
11				26			
12				27			
13				28			
14				29			
15				30			
Poängs Points	summa /	3	Betyg / Grade	Lärarsiç Teache			T, 7.

## Fylls i av tentamensvakt / To be filled in by the invigilator

Antal lösa blad/ No. of sheets submitted	5	Inlämnad tentamen / Submitted exam	Leg kontroll / Control identification	Sign. tentamensvakt / Sign. invigilator
		Försättsbladet akall alltid län	mana in Suan am ingan unnaith babandlata	

Försättsbladet skall alltid lämnas in även om ingen uppgift behandlats Examination cover should always be submitted even if no questions are answered



	Anony	mitetsk	od/ And	nymu	s code:	
5-	0	0	5	-	0	9

				Lärarens anteckning /
1)	NETWO	RK SECURITY	15 THE METHODS THAT	Teachers note:
	CAN REC	COVER, DETECT,	PRE VENT NETWORK SECURITS	
	ISSUES.			
	GENERALL	LY WE HAV	E THREE VECTOR ATTAKS:	
			L NETWORK, REMOTE NETWORK	
			NLY GUAPANTE NETWORK	
			GUARANTEE ALSO	
	SYSTEM	SECURITY,		
	· ATT ACK	prote cted b	Y GUCRY PTION: EAVES & RUPPIN	6
	· ATTACK	NOT POSTECTED &	SY ENCRYPTION: TRAFFIC ANALYS	8,
	MAGQ	VERA DE, REPL	AY, MODIFICATION, DOS	
	· ATTACK	. Protected 1	BY MESSAGE AUTHENTICATION:	
	MASQUE	FRADE, REPLA	4, DOS, EAVES DEUPPING	X
			O BY MESSAGE AUTHENTICATION	
	TRAFFI	C ANALYSIS,	MODIFICATION,	
				- 1



	Anony	mitetsko	d/ Ano	nymı	us code	:
5-	0	0	3	-	0	9

2)	70	E	NCP	- y 1	70	J	1	STI	P F A	M	۵	ΑT	A	0 1		32-	. BIT	È5		rarens achers	anteck note:	ning
	EACH		WE		CAN	)	VS	Е	ç	STR.	EA	W	0 6	LI G	N	ED						
	mode	0	P	01	ERI	A TII	1111 S	L	IKE		l	TR	Ą	NO	l F	В						
	CTR			C R4								De	cry	PΤ								1
	COUNTE	R		Coul	ITER.					CON	NIER	.,		Ī	CONI	ITER	<u> </u>					
¥-	ENCLYP	-	-	ENCA	497	_k			K.	Er	CRYPT	_	- -	-	end	- tap	_ K	<b>\</b>				i i
<sub>F</sub> 4	-			Ø	)P	Ŋ			C4	4	$\phi$		C	<b>)</b> –	-6	)						
	t c i			Ch	J :		-				<u> </u>		1	1	ا , م	<b>.</b> .						
(	FB.			CR	74 y.							DE	CRI	P	T							
	ΙŅ		1							ΙV												1
K_	ENCHALL		KEN	ICHUPT		1		30000000000000000000000000000000000000	K.	-En	ceypt			en	e-upit	-		-				
P <sub>1</sub> .	<del>-</del>		P2_	•	1				N	min (	<del>-</del>	C 1		e		-6 <sub>2</sub>	-					
	C,		(	.2						9	1			PJ								
• (	TR:	5	TRE	A M	- 0	RIE	NTE	٥	, ,	) BP)	+LG	LLI	ZAB	LE		vo	EI	LR OR	٤			
	P	209	AG	ati	9 N	,	NO		GR	AN	T	Αı	ıΤμ	EI	ıtı	(A	tic	) N				
٠ إ	FB:	S	TRE	A M	- 01	LIE A	JTE I	١,.	a 01	ARA	LEI	.bl	ZAB	LE,	۹,	REG	sen	ıt			-	
		EF	er o	D_	P R0	AAI	6AT	10	IN,	,	GR	AN"	٢ .	A V	THE	ENT	101	<b>4</b> 110	Ŋ			
														ļ								
							-							1								
									4													



Anonymitetskod/ Anonymus code: 5 - 0 0 5 - 09

-	2) DECAUSE FUEDIL QUE HAS FASO OTOS DUDIL	Lärarens anteckning /
ŀ	3) BECAUSE EVERY ONE HAS EACH OTHER PUBLIC	Teachers note:
	KEY, WE CAN USE THE DIGITAL SIGNATURE	
	THAT USE HASH FUNCTION MDS IN THOSE TWO	
	METHO 05	
	ETA: APE:	
	PLAINTEXT PLAINTEXT	
		PHVA
KABC	ENCRYPTION KPRIVA PROINTEXT DIGITAL	
	DIGITAL SIGNATURE	
	CIPHELTEXT DIGITAL SIGNATURE KARC	
	SICHATURE CIPERTEXT	
	ONCE THAT A HAS SIGN AND WITH HIS	
-	PRIVATE KEY AND ENCRYPTED WITH KARC SIMMER	4
	REY CAN SEND THE MESSAGE.	
	N.B : THE ENCRYPTION THON AUTHENTICATION (ETA)	-
	METHOD IS ARETERRED BECAUSE THE	
	RECIVER CAN DIRECTY FILTER THE MESSAGE	
	WITHOUT DECRYPT IT IF IT IS COMPROMISED	
	ABC clen't Share public	
	A,B, C clen't share public	key



	Anon	ymitetsko	od/ And	nymu	s code	:
5-	0	0	5	-	0	9

<b>F</b> )		A & G B	Lärarens anteckning Teachers note:
(1)		: A, (A, g no) P	
(2)		: B, CB, 96 MODP, SIGN ( 9 MODP, 9 MODP, CA, CB)	
3	$A \rightarrow B$	A, SIEN ( ga moo A, go moo A, CA, CB)	
6		BOTH A AND B CREATE Kab	
(4)	$A \rightarrow B$ :	A, B, C A SAYS THAT WANT TO CREATE SE CURE CHANNEL WITH ALSO C	A
		A D **	
		KAB (G) KAB	
a		6 76 70	
		A, B, CA, gab MODP	
		C, Cc, g mod P, SIGN ( group, g mod P, CA, Cc)	
_		A, SIGNA (gabman A, gamos P, CA, Cc)	
		B, A, (B, g noop	
		(, (, g' MODP, SIGN (g' MODP, g' MODP, (p), (c))	
ho	8 → (:	B, SIGNE ( gab MODE, ge MODE, CB, CC)	
		EVERY ENTITY A, B, C GENERATE T	HE .
<u> </u>		, Key know for the SELURE CAN	ALINEC



	Anony	mitetsko	od/ Ano	nymı	s code	
5-	0	0	5	-	0	9

5) 9	Lärarens anteckning /
	Teachers note:
$As \longleftrightarrow As \longleftrightarrow$	
B 08	
(9) USER LOG INTO THE WORK STATION WITH HIS PASSWOLD	
The state of the s	
AND SEND TO AS A PLAINTEXT CONTAINING	
A MESSAGE THAT SAYS HE WANT TO CHANGE PASSWOOD	
6) 11000 SOMO A MOSCO OF T(1 (11/ 11/ 11/1))	
2) USER SEND A MESSAGE E(KO, SH(NEWPASS), Na )	
THAT CONTAIN THE NEW HASHED PUBLISH PASSWORD	
THAT CONTINUE THE NEW PASHED PASSWORD	
AND A NONCE, THE'S MESSAGE IS CIPHERED WITH	
THE KEY GENERATED FROM THE OLD PASSWORD	
AND DECRYPT THEM	
3) AS RECEIVE THE MESSAGES , CHECK THE	
USER EXISTS IN HIS DB AND SEND BACK	
TO THE WED A LAGGERAGE ELL (ALL)	
TO THE USER A MESSAGE E(K, {Na})	
CONTAINING THE NONCE, THIS MESSAGE IS ENCRYPTED	
CANTEL WING THE WORLD, THE WE SOUGH IS ENDEMBLED	
USING A KEY GENE RATED FROM THE NEW PASSWORD.	
4) THE USER RECIVE THE MESSAGE, DECAYAT IT WITH	
THE THE DASSING KEY GENERATED FROM THE NEW	
PASS WORD AND TO PROVE THAT HE REQUIRED THE	
TO CHANGE PASSWORD APPLY A TRANSFORMATION	
PREACCORDED TO THE NONCE, ENCRYPT IT WITH	
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1	21
THE NEW KEY AND SEND IT RACK TO AS E(KN) SNOW	4)
	71
(5) AS DECRY PT THE MESSAGE WITH THE NEW KEY	
~~	
CHECK THE TRANSFORMATION AND SAVE THE NEW PASSWOR	0