Mittuniversitetet
MID SWEDEN UNIVERSITY

Försättsblad tentamen / Examination cover

Anonymitetskod / Anonymous code S - 0 0 5 - 0 9		
Kurskod / Course code D T 0 2 4 A	Provkod/ Test code Q 1 0 2	Tentamensdatum / Examination date 2 0 1 8 - 0 2 - 1 5
Kursnamn / Course name Datateknik AV, Nätverkssäkerhet och nätverksdrift		
Provnamn / Test name 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 nedan med X / Mark below with an X		Poäng / Credit	Lärarens anteckningar / Teacher's notes	Markera nedan med X / Mark below 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			
Poängsumma / Points		93	Betyg / Grade A	Lärarsign./ Teachers sign		T, Z.	

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

Antal lösa blad/ No. of sheets submitted 5	**Inlämnad tentamen / Submitted exam** 0	**Leg kontroll / Control identification** ✓	**Sign. tentamensvakt / Sign. invigilator**

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

7698221252

Lärarens anteckning / Teachers note:

1) NETWORK SECURITY IS THE METHODS THAT CAN RECOVER, DETECT, PREVENT NETWORK SECURITY ISSUES.

GENERALLY WE HAVE THREE VECTOR ATTAKS: LOCAL SYSTEM, LOCAL NETWORK, REMOTE NETWORK, SO IF WE CAN ONLY GUARANTEE NETWORK SECURITY WE'LL NOT GUARANTEE ALSO SYSTEM SECURITY.

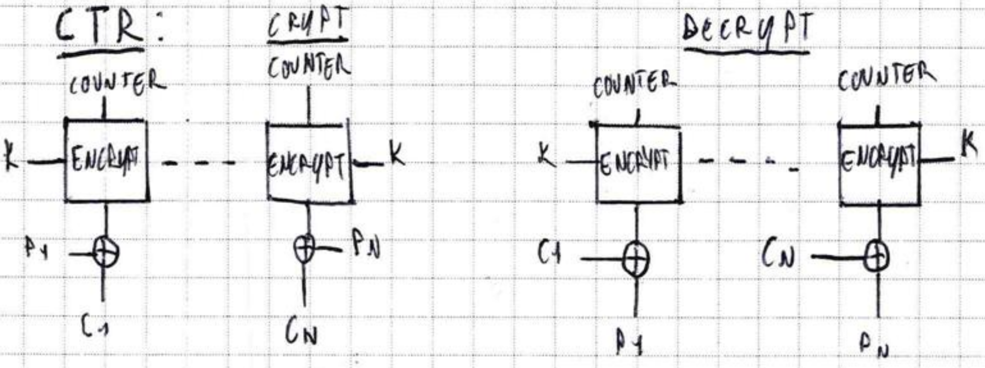
- ATTACK PROTECTED BY ENCRYPTION: EAVESDROPPING
- ATTACK NOT PROTECTED BY ENCRYPTION: TRAFFIC ANALYSIS, MASQUERADE, REPLAY, MODIFICATION, DOS
- ATTACK PROTECTED BY MESSAGE AUTHENTICATION: MASQUERADE, REPLAY, DOS, EAVESDROPPING
- ATTACK NOT PROTECTED BY MESSAGE AUTHENTICATION: TRAFFIC ANALYSIS, MODIFICATION.

X

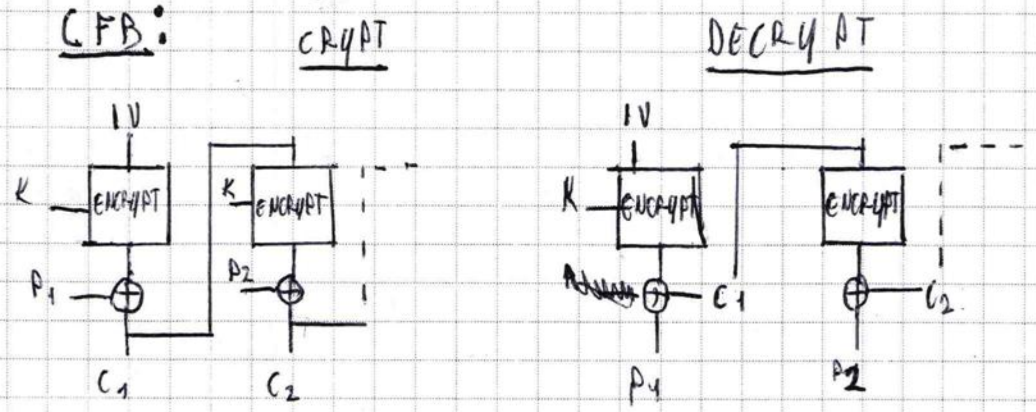
Lärarens anteckning / Teachers note:

2) TO ENCRYPT A STREAM DATA OF 32-BITES EACH WE CAN USE STREAM ORIENTED MODE OF OPERATIONS LIKE: CTR AND CFB

CTR:



CFB:



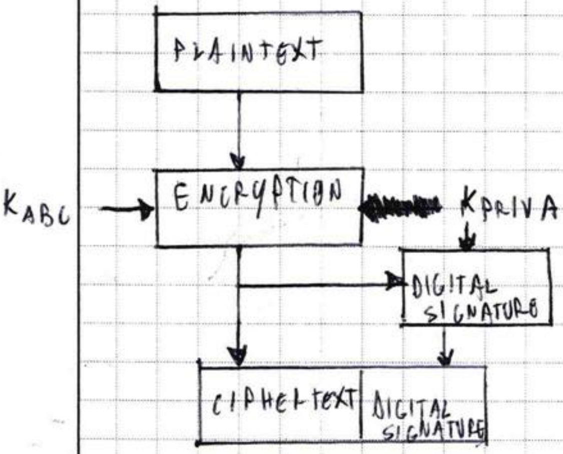
- CTR: STREAM-ORIENTED, PARALELLIZABLE, NO ERROR PROPAGATION, NO GRANT AUTHENTICATION

- CFB: STREAM-ORIENTED, NO PARALELLIZABLE, PRESENT ERROR PROPAGATION, GRANT AUTHENTICATION

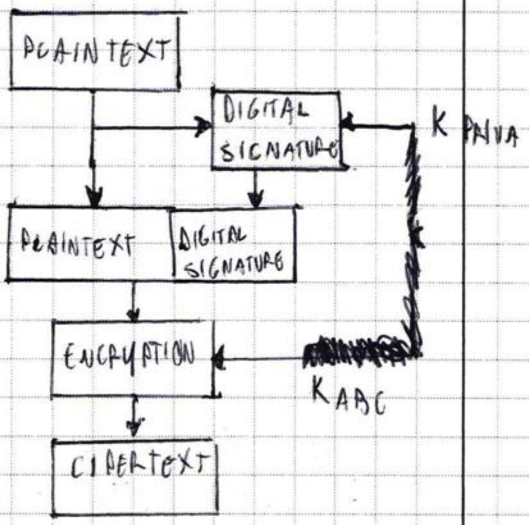
Lärarens anteckning / Teachers note:

3) BECAUSE EVERYONE HAS EACH OTHER PUBLIC KEY, WE CAN USE THE DIGITAL SIGNATURE THAT USE HASH FUNCTION MD5 IN THOSE TWO METHODS:

ETA:



ATE:



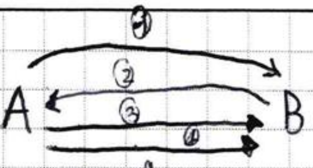
ONCE THAT A HAS SIGN ~~[illegible]~~ WITH HIS PRIVATE KEY AND ENCRYPTED WITH K_{ABC} SIMMETRIC KEY CAN SEND THE MESSAGE.

N.B: THE ENCRYPTION THEN AUTHENTICATION (ETA) METHOD IS PREFERRED BECAUSE THE RECIVER CAN DIRECTY FILTER THE MESSAGE WITHOUT DECRYPT IT IF IT IS COMPROMISED.

A, B, C don't share each other public key

Lärarens anteckning / Teachers note:

4)



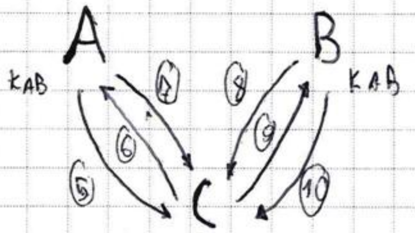
① $A \to B$: $A, CA, g^{a}\ \text{MOD P}$

② $B \to A$: $B, CB, g^{b}\ \text{MOD P}, \text{SIGN}_{B}(g^{a}\ \text{MOD P}, g^{b}\ \text{MOD P}, CA, CB)$

③ $A \to B$: $A, \text{SIGN}_{A}(g^{a}\ \text{MOD P}, g^{b}\ \text{MOD P}, CA, CB)$

BOTH A AND B CREATE K_{ab}

④ $A \to B$: A, B, C A SAYS THAT WANT TO CREATE A SECURE CHANNEL WITH ALSO C



⑤ $A \to C$: $A, B, CA, g^{ab}\ \text{MOD P}$

⑥ $C \to A$: $C, C_c, g^{c}\ \text{MOD P}, \text{SIGN}_{C}(g^{ab}\ \text{MOD P}, g^{c}\ \text{MOD P}, C_A, C_c)$

⑦ $A \to C$: $A, \text{SIGN}_{A}(g^{ab}\ \text{MOD P}, g^{c}\ \text{MOD P}, C_A, C_c)$

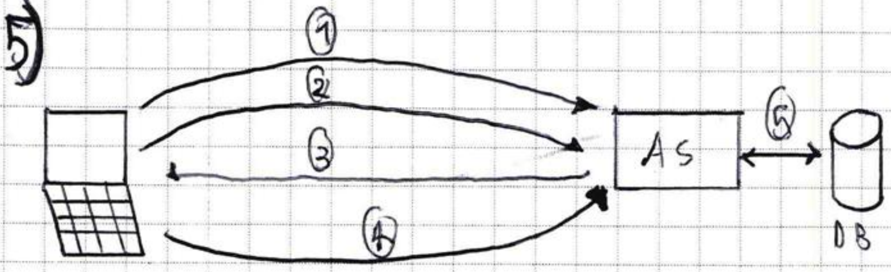
⑧ $B \to C$: $B, A, C_B, g^{ab}\ \text{MOD P}$

⑨ $C \to B$: $C, C_c, g^{c}\ \text{MOD P}, \text{SIGN}_{C}(g^{ab}\ \text{MOD P}, g^{c}\ \text{MOD P}, C_B, C_c)$

⑩ $B \to C$: $B, \text{SIGN}_{B}(g^{ab}\ \text{MOD P}, g^{c}\ \text{MOD P}, C_B, C_C)$

EVERY ENTITY A, B, C GENERATE THE KEY : K_{ABC} FOR THE SECURE CHANNEL

5)



(1) USER LOG INTO THE WORK STATION WITH HIS PASSWORD AND SEND TO AS A PLAINTEXT CONTAINING A MESSAGE THAT SAYS HE WANT TO CHANGE PASSWORD

(2) USER SEND A MESSAGE $E(k_0, \{H(\text{NEWPASS}), N_a\})$ THAT CONTAIN THE NEW HASHED PASSWORD AND A NONCE, THIS MESSAGE IS CIPHERED WITH THE KEY GENERATED FROM THE OLD PASSWORD

(3) AS RECEIVE THE MESSAGES, AND DECRYPT THEM CHECK IF THE USER EXISTS IN HIS DB AND SEND BACK TO THE USER A MESSAGE $E(k_N, \{N_a\})$ CONTAINING THE NONCE, THIS MESSAGE IS ENCRYPTED USING A KEY GENERATED FROM THE NEW PASSWORD.

(4) THE USER RECIVE THE MESSAGE, DECRYPT IT WITH THE ~~NEW PASSWORD~~ KEY GENERATED FROM THE NEW PASSWORD AND TO PROVE THAT HE REQUIRED TO CHANGE PASSWORD APPLY A TRANSFORMATION PREACCORDED TO THE NONCE, ENCRYPT IT WITH THE NEW KEY AND SEND IT BACK TO AS $E(k_N, \{N_a - 1\})$

(5) AS DECRYPT THE MESSAGE WITH THE NEW KEY CHECK THE TRANSFORMATION AND SAVE THE NEW PASSWORD