På tentamen kommer det att finnas två problem där du måste ge definitioner och bevis av satser från listan nedan. Om ditt bevis av en sats använder resultatet av någon annan sats på listan, då måste du bevisa den senare också för att få full poäng (t.ex. beviset av Sats 2.14 i AG använder resultatet av Sats 2.6).

Det blir troligtvis ett par problem till där krävs ett bevis av någonting som är nära kopplat till ett resultat från kursen, inte nödvändigtvis ett från följande lista. I din lösning av ett sådant problem, om du använder någon sats från kursen, så räcker det att indikera, på ett klart sätt, vilket faktum du använder : du behöver INTE bevisa det.

AG Kapitel 1

Ingenting.

AB Kapitel 2

2.1 Definition 2.1, Sats 2.3.

2.2 Lemma 2.5, Sats 2.6.

2.3 MIN definition av SGD(a, b).

2.4 Lemma 2.12, Sats 2.14.

Dessutom : Sats 4.1 från mina tilläggsanteckningar (denna är en starkare version av Lemma 2.11 i boken).

2.5 Sats 2.15, Sats 2.16.

AB Kapitel 3

3.2-3.3 Definition 3.8, definitionerna av *partiell ordning* och *ekvivalens relation*, Sats 3.10.

3.4 Sats 3.11.

AB Kapitel 4

Ingenting.

AB Kapitel 5

Sats 5.24. Dessutom från mina tilläggsantecningar : Satser 3.1 och 3.2.

AB Kapitel 6

6.2 Definitioner 6.2, 6.5.

6.3 Formlerna (1), (2) och (3), s.141-2. Sats 6.7.

6.4 De Moivres formel.

AB Kapitel 7

Sats 7.27.

OBS! Det finns många satser i denna kapitel men både i mina föreläsningar och på de gamla tentamerna har tillämpningen av dessa resultat till lösningen av konkreta problem betonats.

Dock, möjligheten finns för ett tentamensproblem där du måste bevisa någonting kopplat till reultaten i denna kapitel. Då gäller villkoren som jag pratade om ovan.

AA Kapitel 2

Sats 2.2, Definition 2.1, Sats 2.3.

AA Kapitel 3

3.3 Definitioner 3.1, 3.2.

3.4 Sats 3.1.

3.5 Från mina tilläggsanteckningar :

Definitioner 9.1, 9.2, 9.3, 9.4. Props. 9.3, 9.4, Lemma 9.5, Sats 9.6, Korollaria 9.7, 9.8.

3.6 Ni måste kunna procedurerna för att kryptera ett meddelande och för att skriva en digital signatur.