Na zkoušce si každý vylosuje jednu otázku z první půlky semestru a jedu otázku z druhé půlky semestru. Jedna z nich bude poté doplněna početním příkladem.

Otázky obvykle míří na definice, příklady, schémata protokolu či testu a tvrzení označené na přednášce jako „Věta"či „Důsledek"(číslo relevantní věty je uvedeno v závorce). Tato tvrzení budu chtít dokázat za použití technických tvrzení či pozorování (Poznámky a Pozorování z přednášky), u nichž není nutné znát technické detaily důkazů.

Otázka 1:

1. Pojem cyklické grupy a izomorfismu grup. Charakterizace cyklických grup. (1.3)
1. Podgrupy cyklické grupy. Řády prvků cyklické grupy a Eulerova funkce. (1.6)
1. Cykličnost multiplikativní grupy tělesa. (1.8)
1. Popis protokolu RSA.
1. Struktura multiplikativní grupy $\mathbb{Z}_n^*$. (2.3, 2.4)
1. Fermatův test, Fermatovi lháři a Carmichaelova pseudoprvočísla.
1. Rabin-Millerův test, silní lháři a míjení involucí.
1. Odhad počtu silných lhářů Rabin-Millerova testu. (2.8)

Otázka 2:

2. Popis prvočinitelů oboru Gaussových celých čísel. (3.2)
2. Gaussova celá čísla a řešení diofantické rovnice $x^2 + y^2 = z^2$. (3.5)
2. Gaussova celá čísla a řešení diofantické rovnice tvaru $x^2 + y^2 = z^3$. (3.6)
2. Kvadratická rezidua modulo prvočíslo, charaktery a Gaussovy kvadratické součty. (4.5)
2. Ireducibilita racionálních cyklotomických polynomů. (4.7)
2. Jacobiho a Legenderovy symboly a zákon reciprocity. (4.9)
2. Dobré aproximace racionálních a iracionálních čísel. (5.3)
2. Konstrukce a jednoznačnost řetězových zlomků. (5.8,5.10)