V zápočtovém testu budou tři příklady z následujících okruhů:

1. Počítání v Zn – Eukleidův algoritmus, lineární rovnice, umocňování (Euler-Fermatova věta, algoritmus opakovaných čtverců), Čínská věta o zbytcích;

2. RSA šifrování – provoz (výpočet klíčů, šifrování, reziduální dešifrování);

3. Grupy Zn* - řád prvku, hledání generátoru, podgrupy, řešení rovnic x^k=1 (v cyklických i necyklických grupách);

Kalkulačky jsou povoleny pro kontrolu výpočtu, ale nebude bodován výsledek, nýbrž postup podle algoritmu.

Na zápočet je třeba vyřešit test aspoň napůl dobře. V případě neúspěchu je možná jedna oprava na konci semestru.