KRYPTOGRAFIAN ALKEET

4. RÄKNEÖVNINGEN

(1) Alice och Bob använder Diffie-Hellmanns nyckelutbytesprotokoll med primtalet 13 och den primitiva roten 2. Alice väljer 4 och Bob väljer 5 som sin hemliga exponent. Bestäm det gemensamma lösenordet.
(2) Alice och Bob bestämmer sig för att i RSA använda den hemliga exponenten d = lösningen till förra uppgift + 2. Talet n är $1061 \cdot 1163 = 1233943$. Bestäm någon fungerande offentlig exponent e.
(3) Använd Wieners attack för att bryta RSA-uppsättningen i föregående uppgift.
(4) **(Denna uppgift ger 2 poäng)** I Wieners attack antog vi att $0 < e < \varphi(n)$. Hur förändras situationen om vi till talet e lägger till multiplar av talet $\varphi(n)$, och hur många multiplar räcker för att Alices och Bobs RSA-uppsättning inte går att bryta med Wieners attack?
(5) Vad är kvadratska rester och icke-kvadratiska rester? Hur många av båda existerar det modulo p (då p är ett primtal)? För vilka tal a har ekvationen $x^2 \equiv a \pmod 5$ en lösning? Hur många lösningar existerar det i de olika fallen?
(6) För vilka tal x har ekvationen

$$y^2 \equiv x^3 + 1 \pmod 5$$

en lösning y?