MAN 060 – Elementär talteori
Sommaren 2007

ElGamal kryptering

Säkerheten i RSA-systemet vilar väsentligen på förmodan att problemet att faktorisera stora heltal är beräkningstekniskt svårt. Ett talteoretiskt problem som antas vara i stort sett lika svårt är bestämningen av så kallade diskreta logaritmer, det vill säga att hitta *x* i kongruensen $r^x \equiv a \pmod{p}$ där *r*, *a* och *p* är kända, *p* är ett (stort) primtal och *r* en primitiv rot till *p*.

Utifrån denna förmodade svårighet har man skapat en krypteringsalgoritm.
Man utgår ifrån ett primtal *p*, en primitiv rot *r* till *p* samt ett tal *a* med $0 \le a \le p-1$. Talet *a* är den dolda nyckeln; den öppna nyckeln är trippeln (p, r, b) där $r^a \equiv b \pmod{p}$.

Krypteringen sker på följande sätt: som innan separeras klartexten i block och varje block överförs till ett heltal. Låt oss kalla ett sådant heltal *T*.
Välj *k* slumpmässigt med $1 \le k \le p-2$ och bilda

$$\begin{aligned} g &\equiv r^k \pmod{p} \\ d &\equiv T \cdot b^k \pmod{p} \end{aligned}$$

Kryptotexten för *T* blir paret (g, d) där g fungerar som en sorts ledtråd; den innehåller ju ingen information om klartexten.

För att dekryptera (g, d), det vill säga återskapa klartexten *T* vill man beräkna inversen till (b^k) eftersom ju $d \cdot (b^k)^{-1} \equiv T \cdot b^k \cdot (b^k)^{-1} \equiv T \pmod{p}$.
Men $b \equiv r^a \pmod{p}$ så $b^k \equiv r^{ak} \equiv g^a \pmod{p}$. Det räcker alltså att beräkna inversen till g^a som ju är $\equiv g^{p-1-a} \pmod{p}$ och alltså lätt att hitta ***för den som känner a***. (Notera också att man vid dekrypteringen inte behöver känna till *k*.)
Den som däremot vill forcera kryptot kan inte gå denna väg eftersom hon inte känner *a* och antagligen inte heller med hjälp av *b* kan lösa kongruensen $r^a \equiv b \pmod{p}$

Exempel:
Låt $p = 13, r = 2, a = 5$ så att $b = 2^5 \equiv 6 \pmod{13}$. Klartexten benämns som ovan med T, och vi väljer $k = 8$.
Då blir $g = r^k = 2^8 \equiv 9 \pmod{13}$ och $b^k = 6^8 \equiv 3 \pmod{13}$.
Kryptotexten, alltså paret (g, d), blir här $= (9, 3T)$

För att dekryptera beräknar vi först inversen till g^a , det vill säga till 9^5, alltså $9^{12-5} = 9^7 = 3^{14} \equiv 9 \pmod{13}$. Vi skall alltså få klartexten *T* genom att bilda $9 \cdot d$.
Mycket riktigt: $9d = 9 \cdot 3T = 27T \equiv T \pmod{13}$

Självklart skall *p* i ”skarpa” situationer väljas stort, det vill säga ett primtal med hundratals siffror.