cryptographie asymétrique

break point $n=(\sqrt{(n)})^2=(\sqrt{(n_1+d)})^2=n_1^2+2.n_1.d+d^2 \rightarrow 2.n_1.d+d^2 \in \mathbb{N} \quad d \in \mathbb{R}, n, n_1 \in \mathbb{N}$

alice

$alice_d = d \in \mathbb{R}, alice_n \neq n_1 \in \mathbb{N} \quad clefpublicAlice = alice_n.alice_d$

bob

$bob_{n1,} bob_{n2,} bob_{n3,} \in \mathbb{N} \quad clefpublicBob = (bob_{n1}.clefpublicAlice + bob_{n2})^2 \pm bob_{n3}$

alice

perform an exhaustive search to find a whole integer with $x_{alice}, x_{alice\,2} \in \mathbb{N}$ in

$clefpublicBob - x_{alice}.alice_d^2 - 2.x_{alice\,2}.alice_d \in \mathbb{N}$

$clefpublicBob = (bob_{n1}.clefpublicAlice + bob_{n2})^2 \pm bob_{n3}$

$(bob_{n1}.alice_n.alice_d)^2 + 2.(bob_{n1}.alice_n.alice_d).bob_{n2} + bob_{n2}^2 \pm bob_{n3}$

$bob_{n2}^2 \pm bob_{n3} \rightarrow \in \mathbb{N}$

$(bob_{n1}.alice_n.alice_d)^2 - X_{alice}.alice_d^2 + 2.(bob_{n1}.alice_n.alice_d).bob_{n2}$

$bob_{n1}^2.alice_n^2 - x_{alice} = 1$

$(alice_d^2 + 2.bob_{n1}.alice_n.bob_{n2}.alice_d) - 2.x_{alice\,2}.alice_d$

$2.x_{alice\,2} - bob_{n1}^2.alice_n^2 = n_1$

$(alice_d^2 + 2.n_1.alice_d) \in \mathbb{N}$

application numérique

alice

d=sqrt(151)-5

(5+d)^2 =151

2*5*d+d^2 =126

clefpublicealice=7*d

bob

clefpublicbob=(21*clefpublicealice+48)^2-153

alice

clefpublicbob-14102*d-21608*d^2

clefpublicbob-(2*7*__21*48__-10)*d-(__21__^2*7^2-1)*d^2

2277.0000001320

ps: take into account the fact that the creation of an asymmetric cryptographic scheme is one of the most difficult things that I have faced ;**I encourage you to be cautious**