BBB (category: Crypto　points: 136　solvers: 50)

Sometimes I can't distinguish between "b" and "d"

`nc BBB.seccon.games 8080`

解法

固定された暗号文を異なる鍵によって暗号化したものが渡されることがポイント。すべての暗号化におけるeが等しくNの素因数が異なるとしよう。平文をm、各NをN_i $(i = 1, 2, 3, 4, 5)$とすれば、暗号文はそれぞれ$m^e \bmod N_i$ $(i = 1, 2, 3, 4, 5)$となる。これらの暗号文から$m^e \bmod N_1N_2N_3N_4N_5$の値が求まる。ここで、もし$m^e < N_1N_2N_3N_4N_5$であればその値は$m^e$に等しい。$m^e$が求まればmodなど関係なく普通に$e$乗根をとれば$m$を得られる。以上の議論で仮定したのは

1. すべての暗号化におけるeが等しい
2. $m^e < N_1N_2N_3N_4N_5$

の2つである(Nの素因数が相異なることも仮定したが今回の問題ではNの素因数はほぼ確実にバラバラになる)。mが116bytes以下であることとN_iが約2048bitsであることから、第二の条件は

$$m^e \fallingdotseq 2^{896e} < N_1N_2N_3N_4N_5 \fallingdotseq 2^{10240} \longrightarrow e < \frac{10240}{896} \fallingdotseq 11.43$$

となるが、$e \leqq 10$だと拒否されるので$e = 11$であると嬉しい。eの値はこちらが入力するbとseedを使って決められる。`e=rng(e)`を幾度か繰り返すことにより決定されるから、11が`rng`函数の不動点になるようにしたい。11が$\texttt{rng}(x) = x^2 + ax + b \bmod p$の不動点であるとは$11^2 + 11a + b \equiv 11 \pmod p$であることだから、$b \equiv 11 - 11^2 - 11a \pmod p$により$b$を定めればよい。次にseedを決める。毎回11にできれば楽なのだが、mod$p$の下で等しいseedを複数回使うことはできない。よって$\texttt{rng}(s) = 11$や$\texttt{rng}(\texttt{rng}(s)) = 11$などを満たす$s$をseed値として使うことになる。このような$s$が5つ存在するとは限らないが、それなりの確率(実験の結果$\frac{3}{8}$。証明は思いつかなかった)で5つ存在するのでこの方法を使う。まとめると、$\texttt{rng}(11) = 11$となるようにbを決定→ $\texttt{rng}(\ldots(\texttt{rng}(s))\ldots) = 11$なる$s$を5つ見つけてseed値とする→ 5つの暗号文から平文を算出する、の流れでflagを得ることができる。