The Low Exponent Attack on RSA

```
n:=1966981193543797
```

1966981193543797

```
e:=323815174542919
```

323815174542919

```
ifactor(n)
```

37264873 52783789

```
a:=numlib::contfrac(e/n)
```

$$\cfrac{1}{6+\cfrac{1}{13+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{9+\cfrac{1}{1+\cfrac{1}{36+\cfrac{1}{5+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{1+\cfrac{1}{43+\cfrac{1}{13+\cfrac{1}{1+\cfrac{1}{10+\cfrac{1}{11+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{9+\cfrac{1}{5+\ldots}}}}}}}}}}}}}}}}}}}}}}}}$$

```
c:=powermod(2,e,n)
```

838716638068668

```
for i from 1 to 10 do
    k:=numer(numlib::contfrac::rational(a,2*i));
    d:=denom(numlib::contfrac::rational(a,2*i));
    print(numlib::contfrac::rational(a,2*i),(e*d-1)/k);
end_for
```

$\frac{1}{6}$, 1942891047257513

$\frac{27}{164}$, $\frac{53105688625038715}{27}$

$$\frac{27}{164}, \frac{53105688625038715}{27}$$

$$\frac{121}{735}, \frac{238004153289045464}{121}$$

$$\frac{578}{3511}, 1966981103495136$$

$$\frac{6237}{37886}, \frac{12268061702733029233}{6237}$$

$$\frac{1157192}{7029241}, \frac{1138087450659621247239}{578596}$$

$$\frac{3701767}{22485994}, \frac{428312121875354669205}{217751}$$

$$\frac{28456944}{172858711}, \frac{1166130701536020677446}{592853}$$

$$\frac{16257705941}{98755723481}, \frac{31978601836112259330581038}{16257705941}$$

$$\frac{191318803041}{1162145931191}, \frac{376320487552956799050286528}{191318803041}$$

So we get two candidates for phi(n): 1942891047257513 and 1966981103495136. But phi(n) is even, so we try the latter.

```
solve(x^2-(n-1966981103495136+1)*x+n)
```

$$\{[x = 37264873], [x = 52783789]\}$$

Sure enough, this is the factorization of n:

```
ifactor(n)
```

$$37264873\ 52783789$$