An Asymmetric Cryptographic System with Double Key

Jamel Ghanouchi
ghanouchi.jamel@gmail.com

Abstract: We will present in this document a new cryptographic system with double key.

Keywords: Asymmetric, Cryptography, Double Key

1. Approach

1) Bob creates the message.
2) Alice must read it. She makes public two keys: e, e0, two reals and n = p1q1

With p1, q1 two other reals known only by her. Bob sends to Alice C and C0: with MM the integral message and M = log(MM)

C = M^((p-1)(q-1))

C' = M^((p-u)(q-1)+b)

p; q; u; b are known only by Bob with n = pq. But u for which

(p-u)(q-u)(p-1)(q-1) = wC1 = w(p1-1)(q1-1)(p1-u1)(q1-u1)

Alice does not know w. But

\[ e \log(C) = (p-u)(q-u)+b = a \]

\[ e \log(C') = (p-1)(q-1) \]

\[ (p-u)(q-u) = a(p-1)(q-1) - b \]

Let C'' = M^((p-u)(q-u))

But

\[ \log(C) \log(C'') = \frac{ee'}{(p-1)(q-1)(p-u)(q-u)} \log(M)^2 \]

\[ = \frac{ee'}{(a(p-1)(q-1)-b)(p-1)(q-1)} \log(M)^2 \]

\[ = \frac{ee'}{a(p-1)^2(q-1)^2-b(p-1)(q-1)} \log(M)^2 \]

\[ = \frac{ee'}{ae^2 \log(C)^2} - be \frac{\log(M)}{\log(C)} \]

\[ = \frac{e'}{ae \frac{\log(M)}{\log(C)} - \frac{1}{\log(C)}} \log(M) \]

\[ \left( \frac{1}{ae} \log(C'') - e' \right) \log(M) = b \log(C'') \]

\[ \log(M) = \frac{b \log(C'') \log(C)}{1 - \frac{ae}{e'} \log(C'') - \log(C)} = \frac{(p-1)(q-1)}{e} \log(C) \]
\[(p-1)(q-1) = \frac{eb \log(C^c)}{ae} \log(C^c) - e' \log(C)\]

\[(p-u)(q-u) = \frac{wc_i}{(p-1)(q-1)} = a(p-1)(q-1) - b = e' \log(M) - \log(C^c)\]

\[= \frac{ae \log(M)}{\log(C)} - b\]

\[b = \left( \frac{ae}{\log(C)} - \frac{e'}{\log(C^c)} \right) \log(M)\]

But for Alice \(e_0 = f(e)\), \(f\) known only by Alice, then

\[e' = f(e)\]

\[b = \left( \frac{ae}{\log(C)} - \frac{f(e)}{\log(C^c)} \right) \log(M)\]

\[e = g(b, \log(M))\]

\[b = h(\log(M))\]

\[\log(M) = \frac{h(\log(M)) \log(C^c)}{\log(C)}\]

And we have \(M\) if we know \(\log(C^c)\) but

\[w = (p-1)(q-1)(a(p-1)(q-1) - b)\]

\[\log(C^c) \log(C^c) = \frac{ee'}{a(p-1)(q-1)(p-1)(q-1)} \log(M)^2\]

\[= \frac{e^2 \log(M)^2 - \log(M)^2}{ae \log(C)^2}\]

\[= \frac{e' \log(C)^2}{ae \log(C)^2}\]

\[ae \log(C^c) = e' \log(C)\]

\[= \frac{ee'}{a \left( \frac{eb \log(C^c)}{ae} \right)} \log(M)^2\]

\[(p-u)(q-u) = (p-u)(q-u) - b + b = \log(M) - e' \log(C^c) = e' \log(C^c) + b\]

\[e' \log(M) \left( \frac{1}{\log(C^c)} - \frac{1}{\log(C)} \right) = b\]

\[= \left( \frac{ae}{\log(C)} - \frac{e'}{e' \log(C)} \right) \log(M) = b\]

\[= \left( \frac{ae}{\log(C)} - \frac{e'}{\log(C^c)} \right) \log(M) = b\]

\[= \left( \frac{be \log(C)}{ae - e} \right) \log(M) = (p-1)(q-1) \log(C)\]
\[
\log(M) = \frac{h(\log(M))e'\log(C)}{ae'-e}
\]

\[
(p - 1)(q - 1) = \frac{be'}{ae'-e} = \frac{1}{ae} \log(C'') - e'\log(C)
\]

\[
\log(C'') = \frac{e'(-\log(C'') - e'\log(C))}{e(eae'-e)}
\]

And we have \(\log(C'')\) and then \(\log(M)\)

2. **Advantages of the Method**

Comparing to other systems like RSA, the advantage is that we do not work with great numbers, because it is very difficult to identify \(p; q\) knowing \(pq\).

3. **Inconvenients**

It is in the function \(f\) which must be hidden. The challenge is to find one which can not be broken.

4. **Conclusion**

The analytic approach has allowed to put in evidence a new method of cryptography.

**References**
