# An Asymetric 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:** Asymetric, 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 $n = p_1 q_1$
With $p_1$, $q_1$ two other reals known only by her. Bob sends to Alice C and C0 : with MM the integral message and $M = \log(MM)$

$$C = M^{\frac{e}{(p-1)(q-1)}}$$

$$C' = M^{\frac{e'}{(p-u)(q-u)+b}}$$

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

$$(p-u)(q-u)(p-1)(q-1) = wC_1 = w(p_1-1)(q_1-1)(p_1-u_1)(q_1-u_1)$$

Alice does not know w. But

$$\frac{e'\log(C)}{e\log(C')} = \frac{(p-u)(q-u)+b}{(p-1)(q-1)} = a$$

$$(p-u)(q-u) = a(p-1)(q-1) - b$$

Let $C'' = M^{\frac{e'}{(p-u)(q-u)}}$
But

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

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

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

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

$$= \frac{e'}{ae\frac{\log(M)}{\log(C)^2} - b\frac{1}{\log(C)}}\log(M)$$

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

$$\log(M) = \frac{b\log(C'')\log(C)}{\frac{1}{ae}\log(C'') - e'\log(C)} = \frac{(p-1)(q-1)}{e}\log(C)$$

$$(p-1)(q-1)=\frac{eb\log(C'')}{\frac{1}{ae}\log(C'')-e'\log(C)}$$

$$(p-u)(q-u)=\frac{wC_1}{(p-1)(q-1)}=a(p-1)(q-1)-b=\frac{e'\log(M)}{\log(C'')}$$

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

$$b=(\frac{ae}{\log(C)}-\frac{e'}{\log(C'')})\log(M)$$

But for Alice e0 = f(e) ; f known only by Alice, then

$$e'=f(e)$$

$$b=(\frac{ae}{\log(C)}-\frac{f(e)}{\log(C'')})\log(M)$$

$$e=g(b,\log(M))$$

$$b=(\frac{ag(b,\log(M))}{\log(C)}-\frac{f(g(b,\log(M))}{\log(C'')})\log(M)$$

$$b=h(\log(M))$$

$$\log(M)=\frac{h(\log(M))\log(C'')\log(C)}{\frac{1}{ae}\log(C'')-e'\log(C)}$$

And we have M if we know log(C’’) but

$$w=\frac{(p-1)(q-1)(a(p-1)(q-1)-b)}{C_1}$$

$$=\frac{(\frac{eb\log(C'')}{\frac{1}{ae}\log(C'')-e'\log(C)})(a\frac{eb\log(C'')}{\frac{1}{ae}\log(C'')-e'\log(C)}-b)}{C_1}$$

and

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

$$=\frac{ee'}{a\frac{e^2\log(M)^2}{\log(C)^2}}\log(M)^2$$

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

$$ae\log(C')=e'\log(C)$$

$$=\frac{ee'}{a(\frac{eb\log(C'')}{\frac{1}{ae}\log(C'')-e'\log(C)})^2}\log(M)^2$$

$$(p-u)(q-u)=(p-u)(q-u)-b+b=\frac{e'\log(M)}{\log(C'')}=\frac{e'\log(M)}{\log(C')}+b$$

$$e'\log(M)(\frac{1}{\log(C'')}-\frac{1}{\log(C')})=b$$

$$=e'(\frac{a}{\log(C)}-\frac{e}{e'\log(C)})\log(M)=b$$

$$=(\frac{ae}{\log(C)}-\frac{e'}{\log(C'')})\log(M)$$

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

$$\log(M) = \frac{h(\log(M))e'\log(C)}{ae'-e}$$

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

$$\log(C'') = \frac{e'(\frac{1}{ae}\log(C'')-e'\log(C))}{e(ae'-e)}$$

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

[1] Wiener, Michael J. (May 1990). "Cryptanalysis of short RSA secret exponents". *Information Theory, IEEE Transactions on* **36** (3): 553–558.

[2] Håstad, Johan (1986). "On using RSA with Low Exponent in a Public Key Network". *Advances in Cryptology — CRYPTO '85 Proceedings*. Lecture Notes in Computer Science **218**. pp. 403–408