The Da RSA Code

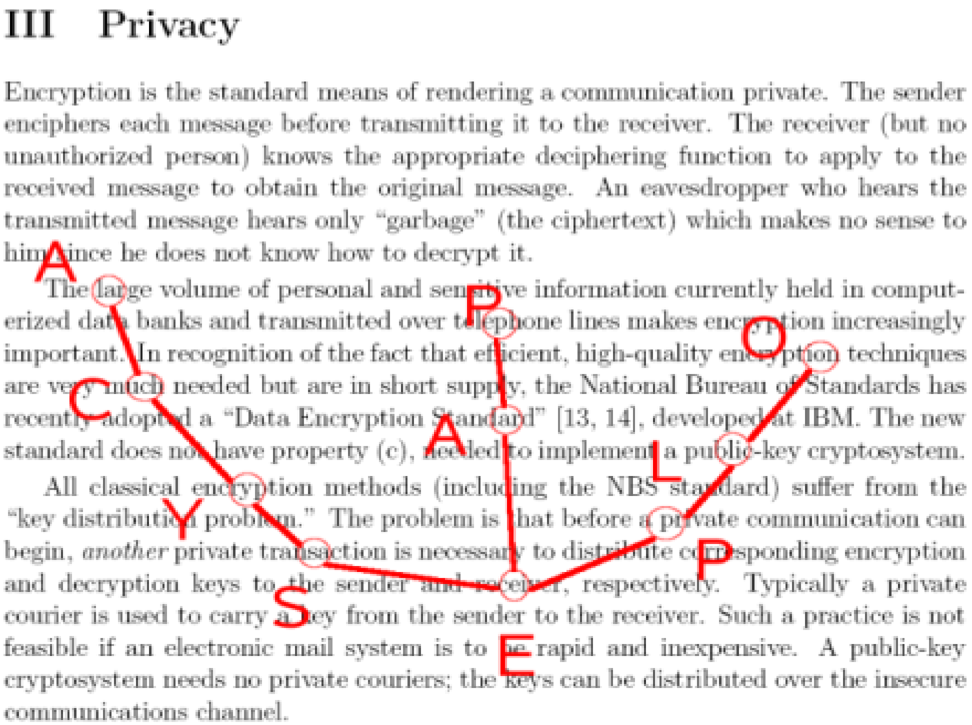
John Saaumson

> *"L'ambition dont on n'a pas les talents est un crime."*
> François-René de Chateaubriand

I Prologue

Since 1970, a lot of people have read the seminal paper of Rivest, Shamir and Adleman, but nobody, as far as we know, has identified the most important message of this article: as this paper demonstrates, cryptical messages are hidden between the lines, using complex Cabalistic techniques (only mastered by experts like Louise Ciccone or Claude Vorilhon), and may deliver fundamental prophecies for the future status of RSA, and cryptology in general. (One might recognize in the title of this paper a reference to two masterpieces of literature, whose erudition and intellectual honesty inspired us for this work.)

II Atomic Holocaust



III Privacy

Encryption is the standard means of rendering a communication private. The sender enciphers each message before transmitting it to the receiver. The receiver (but no unauthorized person) knows the appropriate deciphering function to apply to the received message to obtain the original message. An eavesdropper who hears the transmitted message hears only "garbage" (the ciphertext) which makes no sense to him since he does not know how to decrypt it.

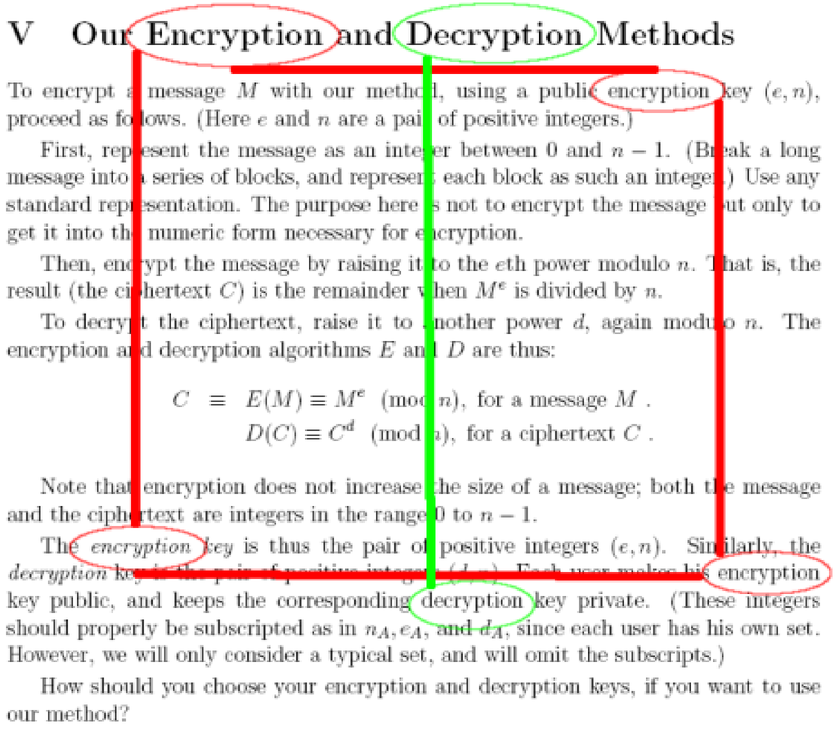
The large volume of personal and sensitive information currently held in computerized data banks and transmitted over telephone lines makes encryption increasingly important. In recognition of the fact that efficient, high-quality encryption techniques are very much needed but are in short supply, the National Bureau of Standards has recently adopted a "Data Encryption Standard" [13, 14], developed at IBM. The new standard does not have property (c), needed to implement a public-key cryptosystem.

All classical encryption methods (including the NBS standard) suffer from the "key distribution problem." The problem is that before a private communication can begin, *another* private transaction is necessary to distribute corresponding encryption and decryption keys to the sender and receiver, respectively. Typically a private courier is used to carry a key from the sender to the receiver. Such a practice is not feasible if an electronic mail system is to be rapid and inexpensive. A public-key cryptosystem needs no private couriers; the keys can be distributed over the insecure communications channel.

Fig. 1. The RSA paper announces Apocalypse.

This first *c*ryptical message is hidden at page 3 of the RSA paper [RSA78]: Figure 1 shows that the Notarikon technique was used to hide the word Apocalypse (from the Greek "apokalypsis", meaning *end of the world*) in the text, by putting a different letter at each successive line, following a mysterious pattern. As our team of experts in gnostic theology revealed (*sic.*), this announces the atomic holocaust between Ma*r*ch 2013 and August 2150.

III The MetaSquare: RSA Will Remain Secure



V Our Encryption and Decryption Methods

To encrypt a message M with our method, using a public encryption key (e, n), proceed as follows. (Here e and n are a pair of positive integers.)

First, represent the message as an integer between 0 and $n - 1$. (Break a long message into a series of blocks, and represent each block as such an integer.) Use any standard representation. The purpose here is not to encrypt the message but only to get it into the numeric form necessary for encryption.

Then, encrypt the message by raising it to the eth power modulo n. That is, the result (the ciphertext C) is the remainder when M^e is divided by n.

To decrypt the ciphertext, raise it to another power d, again modulo n. The encryption and decryption algorithms E and D are thus:

$$C \equiv E(M) \equiv M^e \pmod{n}, \text{ for a message } M\,.$$
$$D(C) \equiv C^d \pmod{n}, \text{ for a ciphertext } C\,.$$

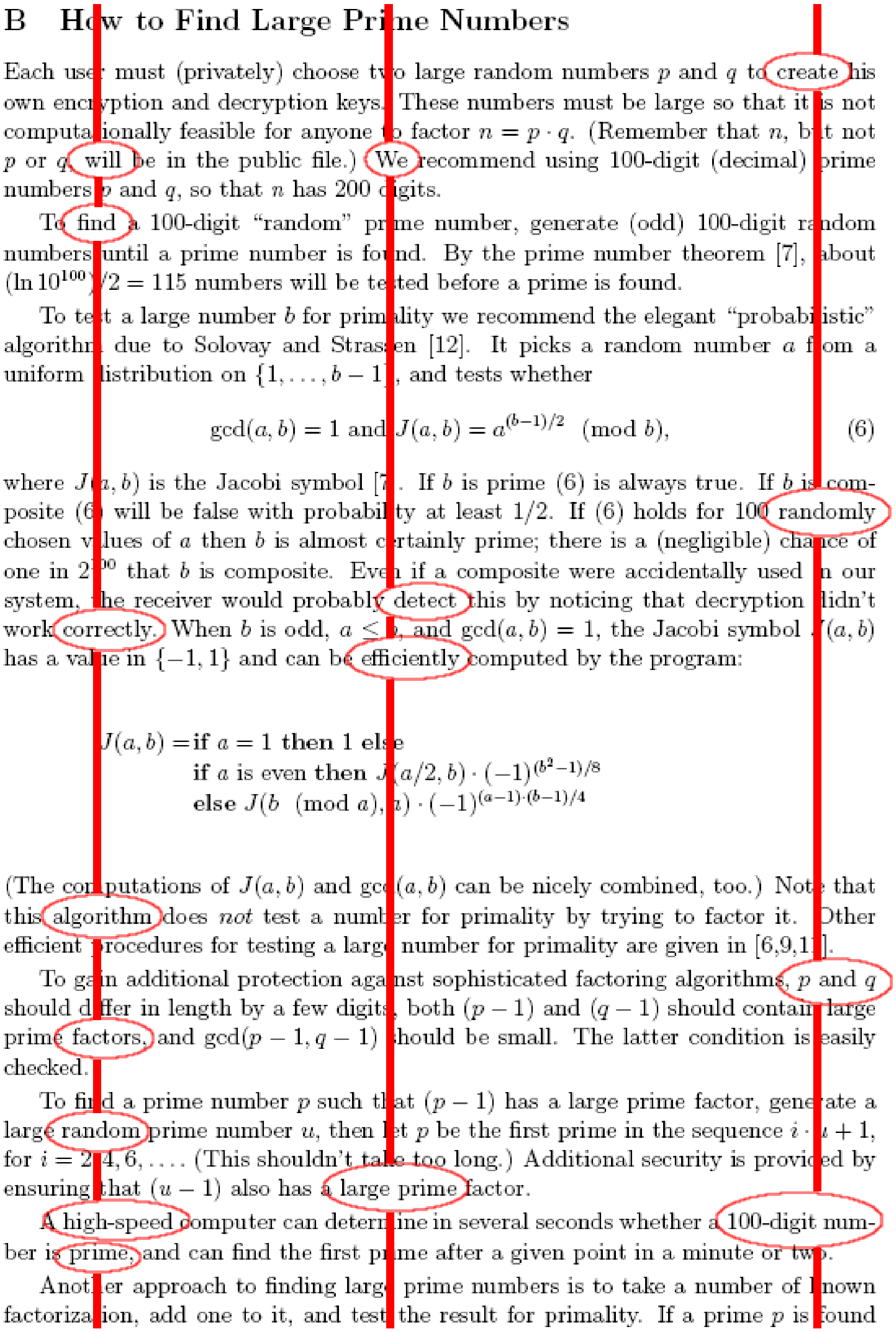
Note that encryption does not increase the size of a message; both the message and the ciphertext are integers in the range 0 to $n - 1$.

The *encryption* key is thus the pair of positive integers (e, n). Similarly, the *decryption* key is the pair of positive integers (d, n). Each user makes his encryption key public, and keeps the corresponding decryption key private. (These integers should properly be subscripted as in n_A, e_A, and d_A, since each user has his own set. However, we will only consider a typical set, and will omit the subscripts.)

How should you choose your encryption and decryption keys, if you want to use our method?

Fig. 2. A perfect Metasquare is drawn by linking the four occurences of the word "encryption", and the two occurences of "decyption" divide the square in two identical parts.

The procedure of *encryption* and *decryption* is described at p*a*ge 6 of [RSA78]. When those two emphasized words are connected by red and green lines respectively, then a strange esoteric pattern appears, as depicted in Figure 2: the formal description of the ci*p*her is surrounded by a perfect square, whose each corner is exactly located on the word "encryption", and the connection of the words "decryption" draws a vertical line, dividing the square in two identical parts. By using some laser measurement technique, it was confirmed that the two parts have exactly the same surface area (with an error margin of $10^{-4}\mu$m).



B How to Find Large Prime Numbers

Each user must (privately) choose two large random numbers p and q to create his own encryption and decryption keys. These numbers must be large so that it is not computationally feasible for anyone to factor $n = p \cdot q$. (Remember that n, but not p or q, will be in the public file.) We recommend using 100-digit (decimal) prime numbers p and q, so that n has 200 digits.

To find a 100-digit "random" prime number, generate (odd) 100-digit random numbers until a prime number is found. By the prime number theorem [7], about $(\ln 10^{100})/2 = 115$ numbers will be tested before a prime is found.

To test a large number b for primality we recommend the elegant "probabilistic" algorithm due to Solovay and Strassen [12]. It picks a random number a from a uniform distribution on $\{1, \ldots, b-1\}$, and tests whether

$$\gcd(a, b) = 1 \text{ and } J(a, b) = a^{(b-1)/2} \pmod{b}, \tag{6}$$

where $J(a, b)$ is the Jacobi symbol [7]. If b is prime (6) is always true. If b is composite (6) will be false with probability at least 1/2. If (6) holds for 100 randomly chosen values of a then b is almost certainly prime; there is a (negligible) chance of one in 2^{100} that b is composite. Even if a composite were accidentally used in our system, the receiver would probably detect this by noticing that decryption didn't work correctly. When b is odd, $a \leq b$, and $\gcd(a, b) = 1$, the Jacobi symbol $J(a, b)$ has a value in $\{-1, 1\}$ and can be efficiently computed by the program:

```
$J(a,b) =$ if $a = 1$ then 1 else
           if $a$ is even then $J(a/2, b) \cdot (-1)^{(b^2-1)/8}$
           else $J(b \pmod{a}, a) \cdot (-1)^{(a-1)\cdot(b-1)/4}$
```

(The computations of $J(a, b)$ and $\gcd(a, b)$ can be nicely combined, too.) Note that this algorithm does *not* test a number for primality by trying to factor it. Other efficient procedures for testing a large number for primality are given in [6,9,11].

To gain additional protection against sophisticated factoring algorithms, p and q should differ in length by a few digits, both $(p-1)$ and $(q-1)$ should contain large prime factors, and $\gcd(p-1, q-1)$ should be small. The latter condition is easily checked.

To find a prime number p such that $(p-1)$ has a large prime factor, generate a large random prime number u, then let p be the first prime in the sequence $i \cdot u + 1$, for $i = 2, 4, 6, \ldots$. (This shouldn't take too long.) Additional security is provided by ensuring that $(u-1)$ also has a large prime factor.

A high-speed computer can determine in several seconds whether a 100-digit number is prime, and can find the first prime after a given point in a minute or two.

Another approach to finding large prime numbers is to take a number of known factorization, add one to it, and test the result for primality. If a prime p is found

Fig. 3. The Transcryptic Lines.

How should we interpre*t* this ? The square is known in many cultures to symbolize Earth and Cosmos (from the Greek "kosmos", meaning *good order* and *secure encryption*), in particular thr*o*ugh the four cardinal points it represents. Also, the square symbols the perfection of Creation, the good order in the Universe, and in Chin**a** is interpreted as a symbol of security, integrity and equilibrium. Therefore, the presence of a perfect square is here to mean that the cipher RSA will bring security and integrity al*l* over the world. The green line of course symbolizes the operation *o*f division.

IV The Transcryptic Lines: Efficient Factorization Will Soon Be Possible

At page 9 of [RSA78] (central symmetric of 6, another multiple of 3!), the section entitled "How To Find Large Prime Numbers" (see Fi*g*ure 3) also reveals surprising messages. When one draws three red vertical lines whose intervals match the divine proportion ($\frac{1+\sqrt{5}}{2}$), each line describes a m*y*sterious message:

1. **"(a) high-speed algorithm will correctly find random prime factors"**: this sounds like the prediction that one will find an efficient algorithm to factorize (here the future is relative to the date of the paper, so the algorithm may already have been found).
2. **"we detect efficiently a large prime"**: this one is mo*r*e subtle to interpret. It can either stand for an elegant synthesis of the achievements reported on the page (large prime can efficiently be found), or this can mean that the large primes can be detected given their product, that is, the so-called RSA modulus. Our teams of semiologists and ling*u*ists are currently working on this question.
3. **"create randomly 200-digit numbers p and q"**: this one is very mysterious, but it may signify that the Creation of universe started with two 200-digit random numbers.

V Conclusion

The most famous paper of modern cryptology conceals several prophecies: we presented here a few examples among the hundred ones we found (which shall be revealed to Mankind in an upcoming novel). It is certain that the presence of such cryptical information is not a coincidence: we looked for ana*l*og messages in a few other papers, and did not find anything, thus the origin of messages in the RSA paper is surnatural. What we learn from the messages revealed here is that:

1. Atomic holocaust will destroy the Universe.
2. As predicts the MetaSquare, the *e*ncryption scheme RSA will remain secure forever.
3. An algorithm exists which factorizes efficiently, and maybe further analysis of the paper will reveal its detail. Our team of midrash exegesists and mathematicians is actually working in this direction.

4. The steganographic process resisted during more than 35 year*s*, we deduce that it is secure, and encourage its use by governments and military services.

Eventually, we encourage such cryptanalysis of the present paper (Mr. Smith [Smi06] may help you for this).

Acknowledgements

We would like to thank Mr. Brown and Mr. Drosnin for their pioneering studies, and Mr. Mc Kay for his brilliant analysis of Moby Dick [McK97],

References

[McK97] Brendan McKay. Assassinations foretold in Moby Dick!, 1997. `http://cs.anu.edu.au/ bdm/dilugim/moby.html`.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.

[Smi06] Mr. Justice Peter Smith. Approved judgement of the case no HC04C03092, between Mr. Baigent and Mr. Leigh, and The Random House Group Limited, 2006. Available at `http://www.hmcourts-service.gov.uk/images/judgment-files/baigent_v_rhg_0406.pdf`.

DISCLAIMER

This paper has been published in the Journal of Craptology, hence it is **not a serious scientific work**, *but instead, in our case, a satirical view of certain best-seller books about pseudo-cryptography and supermarket-esoterism. For this reason, it is voluntarily full of logical non-senses, misinterpretations, and does not aim to reflect the political/theological views of the author, but only parodies the intellectual dishonesty of certain "writers".*