

**JOHN BYRNE**

DESIGN CONSULTANT

P.O. Box C • Rt. 25

EAST CORINTH, VERMONT 05040 • 802-439-6173

March 8, 1991

Mr. Richard Dion  
RD development company  
P.O. box 898  
Bradfor, VT 05033

Dear Mr. Dion:

Perhaps you would like to read the enclosed information about CHAOCIPHER before our meeting on Tuesday morning. It is excerpted from some material written recently by my nephew.

I hope this letter finds you fully recuperated from your recent bout with the flu.

Sincerely,

John Byrne

CHAOCIPHER - THE ULTIMATE ELUSION

Q. What form of input does the cryptosystem accept? [For example, an English language stream, or arbitrary binary data.] What form of output does it produce?

A. In its original form (in the '30s, well before the computer age), CHAOCIPHER was implemented in mechanical form. Like many "elegant" ideas, this was a simple mechanism, but relatively crudely built. It was restricted to the 26 letters of the English alphabet. (Grandpa knew nothing of computers, as you might well guess...and no one else did, either.)

Now, the CHAOCIPHER is enhanced. It will accept input in any digital form. The data may be textual, or binary. CHAOCIPHER produces a binary output file exactly the same size as it's input.

Q. What size restrictions are there on the data that can be encrypted? [For example, any arbitrary bit stream, or data that contains a multiple of 10 characters?]

A. There are no restriction. CHAOCIPHER encrypts data on a byte for byte basis. This means, of course, that the former restriction to the alphabet are lifted, and all 256 combinations of binary data in 8-bit bytes are valid, both as input and output. Furthermore, characters to be encrypted do not have to be grouped, or in any way ordered. Additionally, files to be encrypted may be compressed if desired, before or after encryption, using ANY compression technique. CHAOCIPHER does not, itself, perform compression. It merely accepts character input data and yields character output data.

Q. Is the output produced by encrypting some data the same size as the data?

A. Yes. In its present form, CHAOCIPHER produces an output which is exactly the same size as the input. CHAOCIPHER may additionally contain a modicum of "accounting" information (such as the date/time of encryption). This "accounting" information increases the size of the output file by exactly 9 bytes. The inclusion of "accounting" information is not essential, and may be considered optional.

Here are additional characteristics of CHAOCIPHER:

- o CHAOCIPHER is presently implemented in MS/PCDOS systems. It could easily be converted to run on any platform. In the DOS environment, CHAOCIPHER actually overwrites the original file, using the same disk blocks, with the encrypted file. Since the output file is the same size as the input file, this enhances the security of the process. CHAOCIPHER additionally sets file attributes so that the encrypted files are "hidden" from casual users.

- o CHAOCIPHER is FAST! It has been compared to other encryption systems, and is among the fastest (if not THE fastest) for both encryption as well as decryption. When tested on a TANDY 1000 (8088 at 4mhz) the encryption/decryption rate was approx. 10,000 bits per second. On a TANDY 1000TX (80286 at 8mhz), the rate was 26,200 bits per second. On a DEC Rainbow 100A (8088 at 4mhz) the rate is 8218 bits per second. The CHAOCIPHER program is not yet optimized, and speeds greater than the above may well be realized. Obviously, faster cpu/disk performance than those tested will result in improved performance. Mr. Deavours will complete performance testing on other DOS platforms in the near future.

- o CHAOCIPHER is SECURE. It has NEVER been compromised, and according to Mr. Deavours, is perhaps the most secure algorithm currently available.

- o CHAOCIPHER could quite simply be embedded in other operating systems to provide fast, real time, encryption/decryption of any data stream.

P. 2  
ATT: LAWRENCE MARTIN

AGREEMENT  
by and between

John Byrne  
and  
RD development company

Whereas the aforementioned parties desire to enter into an agreement to produce, market, and sell a computer software package for data encryption implementing the concept currently known as CHAOCIPHER and specifically excluding any source code, John Byrne (JB) of East Corinth, VT and RD development company (RD) of Bradford VT a Delaware corporation so agree to the following:

1. that RD will have the exclusive world-wide marketing and distribution rights of the software package currently titled CHAOCIPHER;
2. that JB will provide to RD all upgrades, fixes, current revision(s) deemed necessary by both parties on a timely basis on written request from RD for corrections/ fixes/ bugs. "Timely" to be agreed upon and dependent on the nature of the project(s);
3. that RD will retain 20% of net sales, that JB will receive 80% of net sales (net sales is defined as that balance of monies after costs and expenses associated with the protection, production, marketing, sales, and support of the product); distribution of proceeds to JB will be on a quarterly basis;
4. this agreement will remain in effect until November 1, 1991;
5. that RD will have the right to extend this agreement with the same terms at the termination date for one year unless it can be demonstrated that RD has not acted in good faith and according to generally accepted good business practice in promoting this product and provided RD can demonstrate serious marketing efforts in a quarterly financial and status report.
6. that this will acknowledge receipt by RD from JB of one computer diskette containing the CHAOCIPHER encryption program and associated files for confidential use in market development for the period ending November 1, 1991. Such development to be consistent with the permanent confidentiality agreement by and between RD and JB of April 17, 1991.

It is further agreed that RD will not provide employment for JB under the terms of this agreement and that JB will retain ownership of said product without recourse by RD.

date: 4/24/91

John Byrne  
John Byrne

Richard Dion  
Richard Dion for  
RD development company

**JOHN BYRNE**

DESIGN CONSULTANT

P.O. Box C • Rt. 25

EAST CORINTH, VERMONT 05040 • 802-439-6173

November 30, 1991

Mr. Richard Dion  
RD development company  
Rt...5 South  
P.O. Box 898  
Bradford, VT 05033

Dear Richard:

As you know, our agreement regarding the marketing and distribution of the software package currently referred to as CHAOCIPHER terminated by its terms effective November 1, 1991.

There was no basis to extend the agreement since neither condition contemplated in paragraph #5 of our agreement for such an extension was met.

I hereby request the return to me of the one computer diskette containing the CHAOCIPHER encryption program and associated files provided to you at the inception of our agreement.

Please call me regarding an appropriate date and time for me to pick up this material.

Sincerely,

John Byrne

A handwritten signature in cursive script that reads "John Byrne". The signature is written in dark ink and is positioned to the right of the typed name "John Byrne".

# R D development company

February 5, 1992

Dear Mr. Burns:

We are in receipt of your letter(s) and phone requests for your material concerning an encryption scheme for use on PC based computers.

In a separate mailing we are packaging all materials due you.

For your information and records, contrary to your beliefs, we contacted approximately 32 different companies/organizations/groups in order to have an evaluation of the material you brought to us. This evaluation was for the purpose of determining the marketability as well as the acceptability of the product concept. In all honesty, our delay in returning the material to you has been based on the fact we had to re-acquire all material(s) that were located at these various locations.

As far as the evaluations that took place, in all instances we were given less than favorable review and all indicated that considerable rewrite of the computer code would have to take place prior to being brought to any market these groups attack. Mainly, the point made centered on the end-user approach taken and the lack of a front end for the users convenience. Further, it appears that there are many products on the market that combine not only encryption but compression as well.

# R D development company

If you believe that no attempt was made on our part, your are mistaken. We expended just a little over \$8,000. in our efforts to develop a potential market and attempt to place the product with a "market-maker." We are not complaining as we assumed a cost would be associated with this effort. Additionally, enclosed with the material being sent to you, are any related materials associated with you 'shower' concept. Again, there are no takers without a sizeable up-front investment which we discussed in the past. We are not willing to provide such and you had indicated the same. The only interest expressed was with a few non-profit organizations but in all instances they only reacted with the concern centered on the cost issues.

Regards



Richard Dion  
for RD development company

seperate packaging

cc: Jay Rosenberg

643-  
Jail  
A