computers the user can be given the feel of one-pass translation through creation of a library of system commands which, when invoked, runs through the multiple operations in response to a short sequence of keystrokes or one click of a mouse.

A C language compiler includes a preprocessor that translates several commonly used directives. The line `#include <math.h>` is an example: it directs the preprocessor to include a *header* file that contains declarations of standard mathematical functions, so that they will be recognized by the compiler if they are used later. The directive `#define PI 3.14159` instructs the preprocessor to replace every occurrence of the string `"PI"` by the numerical value, so that the compiler itself never sees `"PI"`.

Preprocessor operation is very similar to macro expansion, but takes place at an early phase of language translation. Macro languages and assemblers that support a macro facility accept macro definitions as an integral part of language translation and then expand instances of the macro when encountered in the source code. To cope with a language that lacks a macro facility, we can write a preprocessor whose macro definitions are essentially embedded in its parsing logic. The definitions correspond to the syntactical constructs we wish we had in the host language but do not. The preprocessor then detects incoming statements that correspond to these constructs and expands them before the host language translator has a chance to reject them as being ungrammatical.

Edwin D. Reilly

PRETTY GOOD PRIVACY (PGP)

For articles on related subjects, *see* AUTHENTICATION; CRYPTOGRAPHY, COMPUTERS IN; DIGITAL SIGNATURE; ELECTRONIC MAIL; LEGAL ASPECTS OF COMPUTING; PASSWORD; and PRIVACY, COMPUTERS AND.

PGP (*Pretty Good Privacy*) is (1) a program that was popularized in the 1990s for encrypting electronic mail (*q.v.*); (2) a company that was founded by the program's author, Phil Zimmerman; and (3) a trademarked brand of encryption products offered by Network Associates, a US firm that markets computer security software and consulting services.

The PGP program is (partially) based on the RSA data encryption algorithm invented in 1977 by MIT professors Ronald Rivest, Adi Shamir, and Len Adleman. Unlike the symmetric encryption algorithms of the time, which used the same key for encryption and decryption, the RSA algorithm was asymmetric. That is, RSA used one key for encryption and a second key for decryption. For optimal security, both keys had to be based on prime numbers hundreds of digits long (*see* CRYPTOGRAPHY, COMPUTERS IN). The algorithm was published in MIT Laboratory for Computer Science Technical Memorandum #82 (April 1977), and popularized in the August 1977 issue of *Scientific American*. MIT filed for a patent in the fall of 1977 which was issued on 20 September 1983, but the algorithm did not find widespread use because computers of the 1970s were too slow to perform the mathematical operations necessary to implement it.

In 1980, Charlies Merritt, a programmer in Arkansas, discovered a technique for performing RSA encryption on low-cost microcomputers. Merritt's program, *DEDICATE/32*, could encrypt a small file in 20–30 seconds. Unable to find many businesses or consumers interested in the technology, Merritt telephoned computer manufacturers, hoping to find one that would be interested in bundling the product with their systems. He had no success until 1983, when he called Metamorphic Systems, a small computer vendor in Boulder, CO, and spoke with a programmer named Phil Zimmermann. Merritt was unable to convince Metamorphic to purchase the software—Metamorphic was having financial difficulties, and the company soon failed—but Zimmermann and Merritt became close friends. Over the next two years Merritt taught Zimmermann the techniques for performing mathematical operations with large numbers on small computers.

In 1986, Merritt and Zimmermann had their first face-to-face meeting. They were joined by Jim Bidzos, the president of RSA Data Security, a small company that had been created by Rivest, Shamir, and Adleman to commercialize the patented algorithm which they held jointly with MIT. Earlier that year Rivest had created for RSA an email encryption program called MailSafe that used the RSA algorithm. Bidzos demonstrated the program for Merritt and Zimmermann, and left a copy at Zimmermann's house.

After the meeting, Zimmermann decided to write his own email encryption program routine and started on the program in earnest in the spring of 1990. In April 1991 he wrote a letter to RSA asking for a "royalty-free license for your RSA algorithm." Zimmermann needed such a license because he wanted to place his program in the public domain so that it could be used by anyone who felt the need for electronic privacy—especially people who wanted privacy from their own government. RSA refused. Zimmermann nevertheless finished his program during the summer of 1991 and called it *Pretty Good Privacy*.

At about that the same time, the US Senate was considering an omnibus anti-crime bill. At the behest of the FBI, Senator Joseph R. Biden inserted language into the legislation that would have outlawed the use of

encryption systems within the USA that did not "permit the government to obtain the plaintext contents of voice, data, and other communications when appropriately authorized by law." Fearing that use of his program would soon be illegal, Zimmermann gave copies of PGP 1.0 to a few of his friends. One of those friends uploaded the program to a few bulletin board (*q.v.*) systems in Colorado. The program was subsequently republished on the Internet (*q.v.*) and distributed around the world.

Subsequent cryptographic analysis of PGP 1.0 revealed that while Zimmermann's RSA implementation was secure, information encrypted with a second algorithm employed by the product (an algorithm that Zimmermann invented and called Bass-O-Matic) could be easily decrypted. Thus, while PGP 1.0 did provide "pretty good" privacy, it did not provide the military-strength encryption that Zimmermann felt the world needed.

Throughout the fall of 1991 and 1992, Zimmermann guided a team of programmers who had volunteered to rewrite the PGP program and make it a worldwide standard for strong email encryption. One important change was to replace the program's Bass-O-Matic algorithm with a new cipher called IDEA (International Data Encryption Algorithm) invented by Xuejia Lai and James Massey. A second change was to modify the program so that its user interface (*q.v.*) could be easily translated from one language to another, greatly increasing the program's portability (*q.v.*). This program, PGP 2.0, was released on the Internet in late 1992.

In February 1993 the US Customs Department launched a formal investigation of Zimmermann. Although the investigation was originally based on the exporting of a program that violated RSA's patent, the investigators quickly refocused on the exportation of a program that allegedly violated the US laws prohibiting the export of cryptographic software without a license. The investigation was dropped on 11 January 1996.

During the summer of 1993 Zimmermann licensed commercial rights to the PGP program to ViaCrypt, which could legally sell PGP since it already had a license to use the RSA algorithm. But Zimmermann still firmly believed that there should be both commercial and noncommercial, or free, versions of PGP available for all to use. The patent issues for the noncommercial version of PGP were resolved in the spring of 1994. On 14 May 1994, RSA Data Security released a cryptographic toolkit allowing noncommercial use of the RSA algorithm. On 26 May 1994, MIT released PGP Version 2.6, based on the RSA toolkit.

In March 1996 Zimmermann founded PGP, Inc., a new company that would develop and sell a variety of encryption-based products designed to promote privacy. On 1 July 1996, the company acquired ViaCrypt, and along with it both commercial rights to the PGP program and the coveted RSA license. PGP, Inc. went on to develop several new products including a telephone encryption system and a disk-drive encryption program called *PGPdisk*. But despite good technology, PGP, Inc. faltered, and, in February of 1998, was sold to Network Associates, a company formed just a year earlier through the merger of Network General and the McAfee company known for its virus protection software (*see* VIRUS, COMPUTER).

Bibliography

1994. Stallings, W. *Protect Your Privacy—A Guide for PGP Users*. Upper Saddle River, NJ: Prentice Hall.
1995. Garfinkel, S. *PGP: Pretty Good Privacy*. Sebastopol, CA: O'Reilly & Associates.
1995. Zimmermann, P. *The Official PGP User's Guide*. Cambridge, MA: MIT Press.
1995. Zimmermann, P. *PGP: Source Code and Internals*. Cambridge, MA: MIT Press.
1995. Bacard, A. *The Computer Privacy Handbook: A Practical Guide to E-mail Encryption, Data Protection, and PGP Privacy Sofware*. Berkeley, CA: Peachpit Press.
1996. Schneier, B. "Pretty Good Privacy (PGP)," section 24.12 of *Applied Cryptography*, 2nd Ed., 584–587. New York: John Wiley.

Simson Garfinkel

PRINTERS

For articles on related subjects *see* COMPUTER GRAPHICS; DESKTOP PUBLISHING; ELECTRONIC OFFICE; METAFONT; POSTSCRIPT; TEX; TEXT EDITING; TYPEFONT; and WORD PROCESSING.

Introduction

Early predictions that computerized data would lead to the "paperless office" have not been fulfilled. Not only are more printouts than ever before being created, but computer printing has turned into a fine art. The very essence of a whole new category of computing—desktop publishing—is the production of printed pages of ever higher quality.

In the age of the typewriter, there wasn't much you could put on paper except black letters and numbers—most often in an efficient but drab typeface called *Courier*, a "monospaced" font in which all letters have the same width. What forecasters did not foresee was that computer software and printing technology would make possible fast, easy, graphic, colorful hard copies of reports, newsletters, graphs, and, yes, company budgets and greeting cards better than even IBM's best *Selectric*—the state of the art in typewriters before they died—could ever come close to producing.