Text to be appended to the section on irreversible compression

There is another, very practical application for irreversible compression. Living in the digital age, we acquire and use passwords all the time. Imagine buying a new computer. When you run it for the first time, it recognizes you as its owner and asks for a password. The operating system has to save the password, but it is risky to keep the original password in memory or on a disk. The operating system therefore encrypts the password, but what makes this encryption special is the fact that the password will never have to be decrypted! When you log into your computer again, the operating system asks for your password, encrypts the string that you type, and compares it with the encrypted version it has saved.

This is a surprising conclusion. It implies that encrypting passwords is somehow special. In general, when data is encrypted, the encryption algorithm must allow for future decrypting of the data, and this is one reason why encryption methods, even the most modern, secure, and complex ones, are vulnerable and are often broken. An encryption method that does not allow (in principle) for decryption, is unbreakable; it is the ultimate in keeping secrets. Mathematically, such an algorithm is a one-way function.

Traditionally, when this topic is discussed (in lectures or in books on computer security or on operating systems), the modulo function is used as an example. This function is simply the remainder of an integer-by-integer division. Being told that the remainder of $n \div 7$ is 2, implies that n is 2, 9, 16, or any of infinitely many other integers. There is no way to determine n. However, *irreversible compression* is another example of a one-way function that can be used to encrypt passwords.

Want more examples of irreversible compression algorithms? Simple. Just write a book on data compression and you will receive several messages a year with ingenious compression algorithms whose originators forgot to consider the decompression side of things.

Note: When entering a password for the operating system's use, the only risks are (1) someone peeping behind your shoulder and (2) a keyboard stroke logger hidden in your computer. However, when sending a password over the Internet, it has to be reversibly encrypted, so that it could be decrypted and used on the receiving side. Thus, the application of one-way functions (and by implication, of irreversible compression) is very limited.