Rescher, Nicholas. *Leibniz and Cryptography: An Account on the Occasion of the Initial Exhibition of the Reconstruction of Leibniz's Cipher Machine*. Pittsburgh: University of Pittsburgh Library System, 2012. xii + 96 pp. Paper.—In addition to his famously diverse intellectual pursuits, Leibniz was something of an engineer. His most ambitious project in this capacity involved using wind-powered pumps to recirculate the water used to operate machinery in the silver mines of the Harz Mountains. (Despite his best efforts, this project stalled during implementation.) He also designed and built several working prototypes of an innovative calculating machine which employed his idea of a stepped drum (*Staffelwalze*) or "Leibniz wheel." This technology continued to be used in calculating machines for more than 200 years and was also central to Leibniz's idea for an Enigma-like cipher machine that would have essentially automated the process of encoding or decoding messages using a remarkably sophisticated polyalphabetic substitution pattern.

As far as we can tell, Leibniz never actually attempted to build his cipher machine. But he did leave behind some descriptions of the machine, and on the basis of these, together with what is known about the workings of his *instrumentum arithmeticum*, Nicholas Rescher recently commissioned the construction of just such a model. It was unveiled at the University of Pittsburgh's Hillman Library in 2012, and will continue to be on display there until it moves to its anticipated home in the International Spy Museum in Washington, D.C. As its subtitle suggests, the present volume was printed on the occasion of the unveiling of Rescher's model. Unfortunately *Leibniz and Cryptography* cannot be purchased through the usual channels; however, complimentary copies are available upon request from either the author or the University of Pittsburgh Library System. Alternatively, Parts 1 and 2 of the volume, which contain the bulk of its most interesting material, are set to be included in a new, expanded edition of Rescher's *On Leibniz* (University of Pittsburgh Press, 2013).

In Part 1 of this short book, Rescher provides an overview of the nature and source of Leibniz's interest in the theory and practice of cryptanalysis, including his unsuccessful bid to secure an apprentice for John Wallis (1616-1703) with a view to perpetuating the Englishman's remarkable deciphering abilities. In Part 2, perhaps the most interesting part of the book, Rescher offers his account of the inner workings of Leibniz's cipher machine. Part 3 provides a brief pictorial history of such machines and related technologies. Finally, in Part 4 Rescher analyzes some of Leibniz's own relatively scant attempts at decryption.

Leibniz's machine can best be described as resembling a primitive typewriter. In the front it features two rows of keys, one for each letter of the alphabet. Inside the body of the machine there are two cylinders or drums that run parallel to the rows of keys. One of them, the display drum, has a hexagonal cross-section; along each of its six faces the letters of the alphabet are arranged in a different, arbitrary order. When a key is pressed, one of the letters on the display drum is exposed, revealing to the user which output letter corresponds to the input letter. What makes the machine particularly clever is that the display drum periodically rotates, so that the output letter corresponding to a given input letter periodically changes. This rotation is accomplished via the other drum, the activation drum, which connects to the display drum by way of an adjustable stepped-drum mechanism. With each key-stroke the activation drum rotates sixty degrees. The stepped drum then determines the pattern according to which rotations of the activation drum translate into rotations of the display drum. For example, the stepped drum can be set so that the display drum rotates with each key-stroke, every third key-stroke, every other pair of key-strokes, and so forth. This is significant because it allows the user quickly and easily to work with a complex code that anyone without such a machine would find very difficult to crack.

Though there is little of direct philosophical interest in this work, its account of Leibniz’s forays into the field of encryption and in particular its reconstruction of his remarkable machine are fascinating and should hold considerable appeal for those interested in Leibniz’s pursuits more broadly and in the histories of cryptography and machine design. Rescher is to be applauded for undertaking this project.

Stephen Puryear

North Carolina State University