## Please join us for a presentation by

Bill Sherman

From the Cipher Disk to the Enigma Machine: 500 Years of Cryptography

**Thursday, April 23, 2015** 5:30 PM with reception to follow

Pogue Auditorium George C. Marshall Foundation VMI Parade, Lexington, Virginia



## Reservations required by calling Leigh McFaddin at 540-463-7103, ext. 138 or by email to mcfaddinlh@marshallfoundation.org

This event is part of the George C. Marshall Legacy Series sequence on Codebreaking. It is free for members of the Marshall Foundation who show a membership card on arrival. Members will be given priority seating on a first-come, first-served basis. Seating will be limited.

Non-members will be placed on a waiting list when making their reservations and will be charged \$15 at the door if seating becomes available.



## codebreaking

The use of codes in writing can be traced back more than 4,000 years to the Egyptians. The practice of communicating through code did not reach western civilization until the Middle

Ages. During the Renaissance many different methods for making and breaking codes were developed, some of which served as the foundation for modern applications of codebreaking. The invention of the telegraph machine in 1844 reinforced the importance of using codes to communicate sensitive information.

Despite the increasing use of codes until the outbreak of WWI, many countries had not yet begun to organize departments devoted to codebreaking activities. Even after the United States declared war in 1917, the army did not have a program for training soldiers in codebreaking. In the aftermath of World War I many countries, including the United States, continued their codebreaking activities.

At the same time William F. Friedman (*pictured above*) published a series of articles that applied scientific and statistical principles to codebreaking that would serve as the foundation for modern codebreaking. These principles when applied by William Friedman, Alan Turing, and others during World War II, led to the breaking of the Japanese PURPLE code and the Nazi ENIGMA code which gave the Allies a significant strategic advantage in World War II and played an important part in the Allied victory. The code machines developed during World War II operate according to the same basic principles that are used in today's complex codebreaking devices. **Bill Sherman** is the head of research at the Victoria & Albert Museum in London and a professor of Renaissance Studies at the University of York. A visiting professor or



fellow at such renowned institutions as University of London, Folger Shakespeare Library, and New York Public Library, Dr. Sherman has written and spoken about codes, ciphers and the history of espionage. His presentation will include discussion of the controversial idea that William Shakespeare's plays contained secret code.

William Friedman, who became the most important codebreaker in American history, concluded there were no coded messages in Shakespeare's works. Working as a plant geneticist at Riverbank Laboratories, Friedman quickly became drawn into Riverbank's work on codes and ciphers. It was there that he trained codebreaking classes for the U.S. Army. Friedman served on General Pershing's staff in World War I during which time he worked on breaking German code systems and most assuredly would have met George C. Marshall who was also on General Pershing's staff.

As head codebreaker for the War Department, Friedman led a team that broke the Japanese diplomatic code known as PURPLE in 1940. Following World War II, Col. Friedman continued his work in government signals intelligence and became the head cryptologist of the NSA. Upon his retirement from NSA in 1956, he donated his personal papers to the Marshall Foundation where they reside today in the William and Elizebeth Friedman collections. With the announced transfer of Friedman's professional papers from NSA to the Marshall Foundation, the Foundation will become the only organization to have a complete set of Friedman materials.



The George C. Marshall Legacy Series interprets General Marshall's legacy through a multi-year series of events, programs and information centered on key themes, events or episodes. This is a new and unique program that promises substantial benefits to the Foundation and the many constituencies it serves including members, children and families, scholars and researchers, historians and history buffs, and museum visitors of all ages.

Because Marshall's career touched on nearly every major event of the first half of the 20th century, the landscape for the Legacy Series is rich and vast. We will access our own significant resources and collections to create unique activities and events to share with the public. Beginning projects, each lasting about three months, will include Codebreaking, Weapons of War, and Taking Care of the Troops.

Codebreaking	(April—June 2015)
Weapons of War	(July—September 2015)
Taking Care of the Troops	(October—December 2015)

Please see our website for a calendar of events and activities at marshallfoundation.org

GCMF THE GEORGE C. MARSHALL FOUNDATION