DOCID: 3928631 Approved for release by NSA on 12-01-2011, Transparency Case# 63852

The American Revolution's One-Man National Security Agency

There was an American who seems to have been the American Revolution's one-man National Security Agency, for he was the one and only cryptologic expert Congress had, and, it is claimed, he managed to decipher nearly all, if not all, of the British code messages obtained in one way or another by the Americans. Of course, the chief way in which enemy messages could be obtained in those days was to capture couriers, knock them out or knock them off, and take the messages from them. This was very rough stuff, compared to getting the material by radio intercept, as we do nowadays.

This one-man NSA was James Lovell, and besides being a self-trained cryptologist, he was also a member of the Continental Congress. With his cipher designs, Lovell became America's first cryptographic tutor. Unfortunately, his students, the American ministers abroad, though brilliant and talented in political matters, found his systems confusing and frustrating.

James Lovell, born in 1737, studied at Harvard, taught in his father's school in Boston, and became a famous orator. Arrested by the British after the battle of Breed's Hill, he was sent as a prisoner to Halifax in 1776, but soon thereafter he was exchanged and he returned to Boston. Chosen as a delegate to the Continental Congress, he attended the sessions of the Congress beginning in February 1777 and served continuously until the end of January 1782 when he took his only leave. In May 1777, he was appointed to the Committee for Foreign Affairs, where, among other responsibilities, he deciphered dispatches. He became the Committee's most indefatigable member, indeed, sometimes its only active member. Other members arrived and departed, but Lovell stayed on and for five years never visited his wife and children. Before he left Congress in 1782, Lovell had left his mark on American foreign relations and particularly on cryptography.

James Lovell enjoyed the challenge of making and breaking cipher systems. Unfortunately, even learned diplomats of his time had great difficulty understanding his cipher forms completely. For John Adams, the Lovell ciphers caused boundless confusion. As Adams confided in a letter to Francis Dana in Paris in March 1781: "I have letters from the president and from Lovell, the last unintelligible, in ciphers, but inexplicable by his own cipher." In short, Adams could not read Lovell's enciphered dispatches. However, John Adams was not the only diplomat troubled by Lovell's ciphers. In February 1780, Lovell wrote to Benjamin Franklin that the Chevalier de la Luzerne, who had become French minister to the United States the previous year, was anxious because Lovell and Franklin were not corresponding in cipher. Lovell had sent a cipher earlier, but Franklin ignored it. Lovell tried again. In March 1781, Franklin wrote to Francis Dana enclosing a copy of Lovell's new cipher and a paragraph of Lovell's letter in which the cipher was used. Somewhat bewildered, Franklin, accustomed to a simpler cipher, commented: "If you can find the key & decypher it, I shall be glad, having myself try'd in vain."

Lovell's considerable talents for breaking ciphers rewarded Nathaniel Greene and George Washington when enciphered dispatches from the British commander, Lord Cornwallis, were intercepted in 1780 and 1781. Lovell wrote to Washington that he believed the British ciphers were quite widely used among their leaders and urged the general to have his secretary make a copy of the cipher key that he was transmitting to Greene. Interestingly enough, Lovell had discovered a curious weakness in the British cryptographic system: "the Enemy make only such changes in their Cypher, when they meet with misfortunes, as makes a difference of Position only to the same Alphabet." What Lovell

meant was that the same mixed cipher alphabet was merely shifted to another juxtaposition with the plain alphabet.

Lovell got his opportunity to break a critical British dispatch through good fortune. Sir Henry Clinton, commander of the British forces in America, sent an enciphered dispatch via a special courier to Cornwallis. The dispatch explained Clinton's inability to assist Cornwallis with a fleet at Yorktown until a specific day and urged him to hold out. Beached near Egg Harbor, the crew and courier were captured and brought to Philadelphia. It was learned that the courier had hidden the confidential dispatch under a large stone near the shore. Recovered, the dispatch was found to be written in three systems. It took Lovell two days to solve and read the dispatch. The original letter was then sent on to Cornwallis to enable the Americans to use their secret knowledge of the British plans and to counteract them.

James Lovell's secret ciphers produced more confusion than security for American diplomats during the revolution. Only gradually in the years after 1775 did American officials become sophisticated about cryptographic systems. Because of the frustration with ciphers, American statesmen began to rely more heavily upon codes rather than ciphers for secret foreign communications. All of the confusion over the Lovell ciphers provides a remarkable lesson for cipher inventors. Lovell tried to force his system on the best minds of the country—even they didn't understand it, and the system failed.

[This article was adapted from Ralph Weber, *Masked Dispatches: Cryptograms and Cryptology in American History, 1775-1900*, and *The Friedman Legacy: A Tribute to William and Elizebeth Friedman*.]