1116-68-2505 **Gregory V Bard*** (bardg@uwstout.edu), Dept. of Math., Stat., and Comp. Sci., Jarvis Hall Science Wing, Menomonie, WI 54751, and **Theodore McDonough**. *The Two-Time Pad Problem: Plaintext Recovery for One-Time Pads Used Twice.* Preliminary report.

The one-time pad is an encryption scheme used since WWI. It consists of a pad $\vec{k}$, a sequence of independent and uniformly random elements of $\mathbb{Z}_n$, in the possession of both sender and receiver. The sender encodes the plaintext $\vec{p}$ as a sequence from $\mathbb{Z}_n$. Encryption and decryption are addition and subtraction. Specifically, $c_i = p_i + k_i \bmod n$.

While provably secure, the classical proof makes assumptions about the method of use. Each pad ($\vec{k}$) must be used only once—hence the name "one-time pad." It has been known for a while that the cipher can be broken if a pad is used twice. For example, if two ciphertexts, encrypted using the same pad, are intercepted then historical records indicate that it is feasible to recover the plaintexts and the pad itself. This was done in the 1950s at the National Security Agency (NSA) under the codename "VENONA."

However, the method by which it was done has not been published, and is an open area of research. Recovering the two plaintexts is called the "two-time pad problem."

The speaker will highlight some of the interesting mathematical/statistical properties of the two-time pad problem. The talk will be accessible with a moderate knowledge of discrete math. (Received September 22, 2015)