INVITED TALK:

A French Code from the Late 19th Century

David Naccache and Rémi Géraud

École normale supérieure, Paris, France

Abstract

The Franco-Prussian war (1870-1871) was the first major European conflict during which extensive telegraph use enabled fast communication across large distances. Field officers would therefore have to learn how to use secret codes. But training officers also raises the probability that defectors would reveal these codes to the enemy. Practically all known secret codes at the time could be broken if the enemy knew how they worked.

Under Kerckhoffs' impulsion, the French military thus developed new codes, meant to resist even if the adversary knows the encoding and decoding algorithms, but simple enough to be explained and taught to military personnel.

Many of these codes were lost to history. One of the designs however, due to Major H. D. Josse, has been recovered and this article describes the features, history, and role of this particular construction. Josse's code was considered for field deployment and underwent some experimental tests in the late 1800s, the result of which were condensed in a short handwritten report. During World War II, German forces got hold of documents describing Josse's work, and brought them to Berlin to be analysed. A few years later these documents moved to Russia, where they have resided since.

Bio

David Naccache heads the ENS' ISG. His research areas are code security, forensics, the automated and the manual detection of vulnerabilities. Before joining ENS Paris (PSL) he was a professor during 10 years at the Université Paris 2 (Sorbonne Universités). He previously worked for 15 years for Gemplus (now Gemalto), Philips (now Oberthur) and Thomson (now Technicolor). He is a forensic expert by several courts, and the incumbant of the Law and IT forensics chair at EOGN. David is the inventor of 170 patent families and the author of 200 publications in information security and cryptography.

Dr. Rémi Géraud is cryptologist, security researcher, member of the Information Security Group of École normale supérieure. His research interests include the mathematics of public-key cryptographic protocols, information security, physical and network intrusion, defensive design, and on a broader scale the economics and geopolitics of information.