GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Colonel William F. Friedman (The godfather of Cryptology)
"Knowledge is Power"

Robert A. Reeves
October 16, 2000

Prelude

Cryptography – The art and science of "secret writing".

Cryptanalysis – The study of decoding information without the use of a known key.

Introduction

William Frederick Friedman (1891-1969) was the chief cryptanalyst of the War Department in Washington D.C. from 1941 to 1947. His original name was Wolfe Friedman, and he was born on September 24, 1891 in Kishinev Russia. He changed his name to William when the family immigrated to America in 1891. Friedman began working with cryptology in his spare time while attending college at Cornell University while working on a degree in genetics. In 1917, due to his amazing success in breaking codes, he became the head of the Department of Ciphers.

During this time period, America became involved in WW I. Encrypted messages that were intercepted where given to Friedman to decipher, he was successful in decrypting every one. In the 1920's, he became the first person to apply mathematical principals to cryptology. During this same time period, mechanical machines were invented, which had multiple rotor parts, thus producing more complicated and complex codes. Friedman began using mathematics to reconstruct these complex machines which enabled him to decrypt even the most complicated codes produced.

Throughout the 1930's, Friedman continued to break even the most complex of codes. During WWII he and his staff worked secretly at breaking the enemy code. In 1941, code that was being secretly sent from Japan to Japanese officials in the U.S. was sent to Friedman and his staff for deciphering. These complex codes could be quickly deciphered due to Friedmans invention of "The Purple Machine" (given its name from the Purple cipher in which the Japanese messages were exchanged). Copies of the machine were also given to the British enabling them to decode messages sent between Japanese officials and Nazi Germany.

The Purple Machine

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Purple was the newest ciphering method used by the Japanese during WW II. In Japan, Purple was titled 97-shiki 0-bun In-ji-ki, which means alphabetical typewriter 97. The number 97 came from the Japanese calendar year 2597 (which is the same as 1937). Purple consisted of two electric typewriters that were linked with a six-level, twenty-five point telephone exchange device. The telephone mechanism had stepping switches and a plugboard, which enabled various cipher keys to be arranged. The enciphering process began on one of the typewriters. Each key on the typewriter keyboard connects to a wire, which links to a switchboard. It had twenty six holes lettered A to Z and a wired plug attached to each hole. As electrical impulses are received from pressing the typewriter keys, they are re-routed and sent on to different destinations by rearranging the plugs on the keyboard. In order to confuse the enemy, the Japanese would move the plugs daily, much like they daily crypto updates of today. The letter A already changed in to a D, by the plugboard travels along the D wire into the box of cipher wheels. Each wheel represents a different letter and each disc has twenty-six letter of the alphabet in scrambled order written around the edges. The original A which is now a D, after the plugboard travels to the wheel standing in the D position. It can now represent another letter, for example the letter P. If P is represented, then the second typewriter will print P. After P has been typed, the cogs turn a certain number of spaces and the next time A is typed it may come out as S, T. or M. The result of this is a word being able to be encoded in thousands of variations.

The Purple Cipher Machine had three different forms, which were classified as Type A, Type B, and Type C. Type A systems were not very complex. The text was mostly in English. This type of cipher was normally used for routine matters and everyday administrative type traffic. Type B dealt mostly with economic matters throughout the world and was used mostly by Japanese officials who were knowledgeable with world economics. Type C systems had the highest level of traffic with between 50 to 100 messages sent daily. Ciphers sent through Type C were encrypted using the Roman alphabet. This text was called romaji. Romani was very complex and extremely challenging to break.

In 1941, Friedman and his staff were able to build a close replica of the purple machine, enabling America to decipher the encrypted codes being sent by the Japanese. The process in which Friedman and his staff were able to decipher the Japanese code was so amazing, it was nick named "Magic".

Magic

MAGIC received its name from Friedman because he referred to his staff of crytpanalyists working on the ciphers as magicians. Friedman and his staff of

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

"magicians" were responsible for reconstructing the Purple Machine and eventually cracking the Purple Cipher. After twenty months of working on cracking the Purple code, in 1940, Friedman and his staff were able to crack the code. One of the main reasons it took so long to crack was due to the Japanese replacing versions of the code once it was know that it has been compromised. The messages sent by Purple would take weeks and sometimes month to decipher, a tedious, and sometimes frustrating task taken on by Friedman and his staff.

MAGIC was instrumental in the interception of key messages transmitted from the Japanese to the NAZI's in WW II. Messages containing Hilters capabilities and plans, as well as, detailed military data were intercepted and decrypted by "MAGIC". The day before the attack on Pearl Harbor, cryptanalysis had decoded the message that the attack was about to take place. The message was available in Washington DC the day before the attack, but the Americans were busy reading ciphers and working on solving other systems at the same the time message was received. It became clear after the attack had taken place that the warnings of the imminent attack were in hand. Following this incident, the importance of speed in the deciphering process became apparent. Translation speeds were increased from an average of 4.6 days to 2.5 days. Greater emphasis was also placed on the importance of each message.

Conclusion

Colonel William Friedman is just one of many notable personalities who participated in the evolution of Cryptography, he is in the company of Julius Caesar, Sir Francis Bacon, and Thomas Jefferson, just to name a few. Colonel Friedman went on to become a key cryptologist of the Department of Defense. In 1964 President Harry Truman awarded him the Medal of Merit, which was the highest Presidential civilian award. He retired in 1955. He died in Washington DC on November 12th, 1969 and is buried in Arlington National Cemetery. He is still known as the greatest cryptologist of all time. His epitaph reads "knowledge is power".

Sources:

Arlington National Cemetery Website
http://www.arlingtoncemetery.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

CME's Cryptography Timeline
http://world.std.com/~cme/html/timeline.html

History of Cryptography
http://emmy.NMSU.Edu/~crypto/History.html

The Science of Cryptology
http://emmy.nmsu.Edu/~crypto/

Kurzeja, Karen. "Pearl Harbor &Ciphering Methods
http://raphael.math.uic.edu/~jeremy/crypt/contrib/kurzeja.html

Kong, Lilian. "The Purple Machine"
http://raphael.math.uic.edu/~jeremy/crypt/contrib/lkong1.html

McLaren, Amanda. "Purple Cipher Machine", 1995
http://shakti.trincoll.edu/~rmorelli/FYSM122/docs/amanda.html

Daoudi, Walteed. "William Friedman"
http://raphael.math.uic.edu/~jeremy/crypt/contrib/daoudi2.html

William Friedman
http://norfacad.pvt.k12.va.us/project2000/friedman/index.htm

Hebert, Shireen J. "A Brief History of Crytpography"
http://www.cybercrimes.net/Cryptography/Articles/Hebert.html

© SANS Institute 2000 - 2002 Author retains full rights.

Robert A. Reeves
October 17, 2000

Colonel William F. Friedman (The godfather of Crytpology) Questions

True/False

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. Q. Crytanalysis is the study of decoding information with the use of a known key.

   A. False. Crytanalysis is the study of decoding information without the use of a known key.

2. Q. Cryptography is known as the art and science of "secret writing".

   A. True.

3. Q. Colonel Friedman attended Cornell University in order to study cryptography.

   A. False. Colonel Friedman attended Cornell University in order to get a degree in Genetics, and worked with cryptography in his spare time.

4. Q. During WWI encrypted messages given to Friedman and his staff were unable to be decoded.

   A. False. During WWI Friedman and his staff were able to successfully decrypt every message given to them for decoding.

5. Q. Colonel William Friedman is the inventor of "The Purple Machine" used to decode encrypted messages during WWI and WWII.

   A. True.

Multiple Choice

1. The Purple Machine was given its name from:

   a. Color of ink in the Typewriters used during that time frame.
   b. The name of the inventor was William Purple.
   c. The method of ciphering used by the Japanese during WWII was called Purple.

2. The Purple Machine had three different forms, they were called:

   a. One, Two, and Three
   b. A, B, and C
   c. unclassified, confidential, and secret

3. The art and science of "secret writing" is known as:

   a. Cryptography
   b. Cryptanalysis
   c. Crypto

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4. One of the main reasons it took so long to crack the Purple Cipher is:

   a. The messages were encoded using the Japanese language.
   b. Colonel Friedman and his staff were under-manned.
   c. The Japanese replaced compromised versions of the code.

5. The encoded message about the attack on Pearl Harbor, sent from the Japanese was available in Washington D.C. how long before the attack took place?

   a. 1 week
   b. 1 day
   c. 1 hour

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.