Threat Against Hack.lu

Hack.lu 2009 Crypto Challenge

The Hack.lu Team

Hack.lu 2009

The Challenge

- Experimenting cryptanalysis in a real context with quite realistic contraints.
    - Time.
    - Cryptogram size.
- Making it a little bit more funny than simply giving cryptograms to decrypt.
- The 3-step scenario is very close to real cases (1996, 2001 and 2006).
- A technical debriefing paper will be published after Hack.lu.

The Scenario

- Two terrorist teams acting in parallel.
    - Team A for the logistic support.
    - Team B for the terrorist attack itself.
- Terrorist teams are communicating through encrypted messages. Two kind of cryptosystems
    - Manual tactical system (step 1). Custom officers must not be suspicious at the airport.
    - "Modern" tactical stream cipher embedded in executable or anything else (steps 2 and 3).
- The challenge is then an interesting mix of crypto and sexy hacking tricks.

Step One

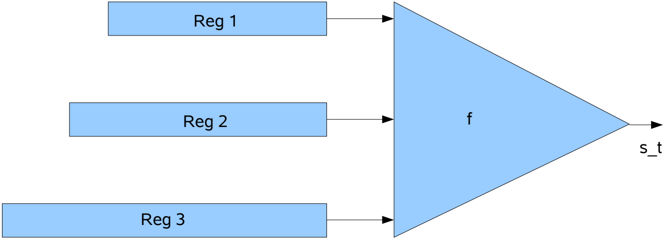
- Simple transposition cipher.
- Key : `THEALMIGHTYVSHACKERS`.
- The message :

> *Glory to our God. May the Almighty be with us, my brother, to eradicate the western infidels's technology and prevent them to enslave us, we and our brothers. Death to hackers who penetrate our networks. You have to beware of everybody here. This country is unfriendly. A room has been reserved for you at the hotel which has been said before your departure. You stay there until the attack. Be as discreet as possible. Your instructions for our operation await you in a special location where you can pick them up securely. It consists in a geocache (geographical hidden place) which in fact is a box you will find located at the following coordinates : 40 degrees North 38,422 minutes, 6 degrees East and 9353 minutes. What is contained in that box will tell you how to conduct the operations. Be cautious with its content since you will have a single occasion to access it. Give the secret key and read. Good luck my brother and may the Almighty be with you.ENDOFTEXT.*

Step Two

- Intelligence show that Taliban AntiHackers have developped their own system.
- Stream ciphers of 59-bit key.
    - Sufficient for tactical purposes.
- Very simple cryptographic primitives
    - Three LFSRs.
    - A Boolean combining function.
- There exist weaknesses to exploit.
- Operational use of that system still unknown.

The Taliban AntiHackers Cryptosystem



The Taliban AntiHackers Cryptosystem

Linear feedback shift registers are given by :

$$P_1(x) = x^{17} \oplus x^{15} \oplus x^{14} \oplus x^{13} \oplus x^{11} \oplus x^{10} \oplus x^{9} \oplus x^{8} \oplus x^{6} \oplus x^{5} \oplus x^{4} \oplus x^{2} \oplus 1$$

$$P_2(x) = x^{19} \oplus x^{18} \oplus x^{16} \oplus x^{15} \oplus x^{11} \oplus x^{10} \oplus x^{5} \oplus x^{3} \oplus x^{2} \oplus x \oplus 1$$

$$\begin{aligned} P_3(x) &= x^{23} \oplus x^{22} \oplus x^{21} \oplus x^{20} \oplus x^{17} \oplus x^{16} \oplus x^{15} \oplus x^{12} \\ &\oplus x^{10} \oplus x^{8} \oplus x^{7} \oplus x \oplus 1 \end{aligned}$$

The combining function is given by :

$$f(x_1, x_2, x_3) = x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3.$$

Scenario Timing

Everything is on the website. Stay stunned !

- Night Oct. 27th to Oct 28th. Find the USB key in the geocache and copy it (be wise !).
- Oct. 28th (morning). Plaintext 1 released and USB key image available on the website.
- Oct. 29th (noon). Solution to step 2 released and hint for the step 3.
- Oct. 30th (14th). Bombing or not bombing ?
- Oct. 30th (4pm). Results and award ceremony.

Conclusion

- Thanks to Anthony Desnos for the support.
- Good luck guys.