M
Chief of Secret Intelligence Service
MI6

Classified Top Secret

Dr. Q
Chief Technology Scientist
Secret Intelligence Service

Dear Dr. Q,

We have just got information that Sicarra and allies have broken all cryptographic ciphers we use. You and your interns are requested **to design a new block cipher** for special agent 007's secret operation at an undisclosed location. The block cipher should **encrypt 32 bit blocks** at a time and should be tested and delivered to us by **20th March 2016**. Please submit the following by the deadline. **World peace depends on it!!!**

1. **Well commented encryption program in C (or/and) assembly, optimized for 32 bit Intel x86 platforms**
2. **Well commented decryption program in C (need not be optimized)**
3. **A document answering the questionnaire included in this letter**
4. **Any other programs / scripts that you wrote during the cipher design (for instance to generate the linear approximation table or the s-box non-linear equations). Does not have to be in C.**
5. **Readme on how to run the codes**
6. **Makefile for compiling the codes**

Regards,

M

PS 1: It is highly recommended that you write codes in a 32 bit Ubuntu 14.04.3, using a virtual box if needed. The image can be downloaded from http://www.ubuntu.com/download/desktop. Use standard gcc compilers.

PS 2: Use the questionnaire to guide you through the cipher design

M
Chief of Secret Intelligence Service
MI6

Classified Top Secret

Questionnaire

Section 1 (to be submitted by March 1st 2016)

1. What is your cipher called?

2. How many rounds does your cipher have?

3. Explain one round of your cipher. You can assume that key expansion is done by a separate process. Don't need to explain that. You can assume that your encryption function takes an array of N keys, where N is the number of rounds in your cipher.

4. How did you arrive at the number of rounds for your cipher?

5. How did you choose the s-boxes size and type?

6. How did you go about choosing the s-box(es) mappings?

7. For your s-box(es), explain / demonstrate how you satisfied the following properties

    a. The balancedness property
    b. SAC
    c. Non-linearity
    d. Algebraic degree (optional)

8. Draw the linear approximation table for your s-box(es).

9. Draw the differential distribution table for your s-box(es).

10. How did you choose the diffusion layer for your cipher?

M
Chief of Secret Intelligence Service
MI6

11. How many rounds would it take to obtain complete diffusion? Show minimum rounds needed for diffuse completely when the i-th bit in the plaintext is toggled, where i can vary from 0 to 31.

Section 2 (to be submitted by March 10th 2016)

12. Show formally and with figures and code, the most deadly linear trail in your cipher. Ensure that an attacker would find linear cryptanalysis more difficult than brute force.

13. Show formally and with figures and code, the most deadly differential trail in your cipher. Ensure that an attacker would find differential cryptanalysis more difficult than brute force.

14. Revsit all questions in Section 1. If you decide to make changes in any of the answers, mention them here and justify why you are making the changes.

Section 3 (to be submitted by March 20th 2016)

15. Have you thought about efficient implementations? If so, demonstrate and document tricks in software and cipher design choices that have makes your cipher efficient to implement on the target platform.
    (you can either choose to optimize to take minimum memory or minimum operations)

16. Revisit all questions in Section 1 and Section 2. If you decide to make changes in any of the answers, mention them here and justify why you are making the changes.

17. For files of sizes 2^n, where n=5 to 20, plot the file size vs the encryption time on the target platform (Intel 32-bit x86).

18. Demonstrate the working of your cipher. Encrypt file alice.txt and save the result in enc_alice.txt. Decrypt enc_alice.txt and save the decrypted result in dec_alice.txt.

**** Answers should be supported by neat figures and code used for finding results. Credit will be given for innovation.