## Cellular Automata in SM4

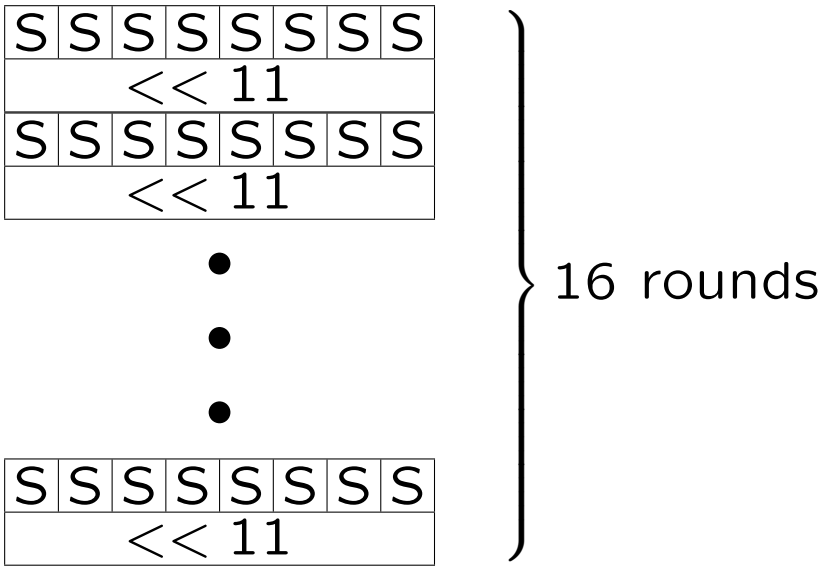
Two cellular automata are used in SM4, one in the encryption process and one in the key schedule. Determine whether these cellular automata are invertible.

You may either approach this problem theoretically or approach it experimentally by programming the automata and running them on the four-billion 32-bit words and testing for invertibility.

IFF and Adaptive Chosen-text Cryptanalysis

Your are operating an intercept radar that is posing as a fire-control radar, challenging aircraft to identify themselves. You send challengs to hostile aircraft and analyze their responses.

The aircraft are using a 32-bit block cryptosystem of the following form

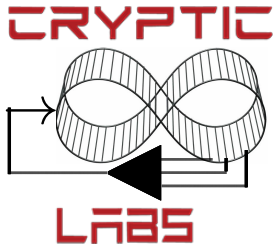



in which the round function is the feedback function from Magma, using only one s-box rather than eight. It is keyed by the contents of its s-box. You are trying to break the system so that your own aircraft can respond to challenges from the opponent.

- If the s-box were arbitrary — entries selected at random with replacement — it would contain 64-bits of information but the encryption would not be invertible. What is the expected number of distinct outputs of such a random s-box. What is the number of distinct output of the encryption system after $n$ rounds.

- If the s-box is invertible but otherwise selected randomly — entries selected at random without replacement — how many bits of information does it contain?

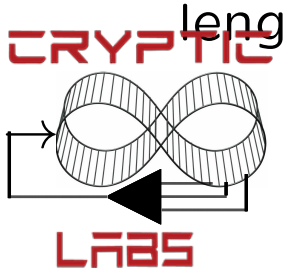
- You may approach these questions either theoretically or experimentally.






Suppose that an invertible s-box has been chosen and the IFF cipher has only one round — eight 4-bit substitutions followed by a rotate 11 to the left. Describe how you would break it (recover the s-box) if you could make an arbitrary numer of requests to the aircraft to encrypt challenges of your choosing. What might you discover from a single request for encryption of a chosen value?

Suppose you have managed to get the aircraft to send you the result of a 16-round encryption of a block of 32 zeroes and the result of a 15-round encryption of a block of 32 zeroes. How would you use this to allow you to attack the single-round cipher described in the paragraph above. How would you arrange to get the aircraft to send you a 15-round encryption of a challenge?

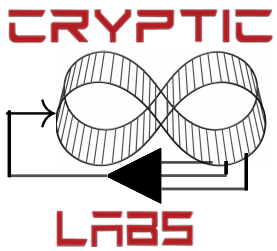





## Variations on RSA

- Suppose that you were to consider employing the RSA cryptosystem with the modulus 35. What is wrong with that modulus other than the fact that it is much too small?

- Examine the smallest possible RSA moduli: $6 = 2 \times 3$, $10 = 2 \times 5$, up through perhaps $143 = 11 \times 13$, $323 = 17 \times 19$ or even $899 = 29 \times 31$. What is the smallest of these that exhibits the attractive properties of the RSA system, for example, keys should not be their own inverses. (In class, I used $77 = 7 \times 11$. Is that a good tutorial choice? Can you find a better one?)






- Suppose you were to build an RSA-like system in which the modulus had three prime factors rather than two. What would $\phi(p \times q \times r)$ be? Would this be a good idea or not? Why? What would be the impact on the sizes of the primes you needed to use.

- Suppose you were to build an RSA-like system in which the modulus had four prime factors rather than two. What would $\phi(p \times q \times r \times s)$ be? This system would suffer from some of the same problems as the 3-prime system discussed above but it has been proposed for some applications because two parties could each know two of the factors without being able to factor the modulus. For what might this be valuable?