The art of cryptography: cryptanalytic world records

10. Assignment: Permutation-based cryptography
(Due: Friday, 20 June 2014, 12:00)

Exercise 1 (inverting SPNs). (Baby-)AES has the following structure:

- AddRoundkey
- For $i = 1 .. R$ rounds repeat:
  - SubBytes
  - ShiftRows
  - MixColumns (omit in round $R$)
  - AddRoundkey

(a) (5 points) Show that decryption of (baby-)AES can be achieved with a similar structure using modifications AddRoundkey', SubBytes', ShiftRows', MixColumns' instead of their "originals". (Hint: ShiftRows and MixColumns of baby-AES are self-inverse and the key schedule is invertible.)

(b) (3 points) Repeat the exercise above for a general SPN-network with omitted Permutation in the last round.

(c) (3 points) Repeat the exercise for a Feistel-Network, where the flip in the last round is omitted.

Exercise 2 (your implementation of baby-AES). For 3-round baby-AES as discussed, you should implement two functions.
(a) (5 points) Write a $\text{enc}(x, k, i)$ which computes the state of AES after round $i$ of our 3-round AES given a message $x$ and key $k$. In other words $\text{enc}(x, k, 0)$ should return $x + k^0$ and $\text{enc}(x, k, 3)$ should return $\text{aes}(M, K)$. Print $\text{enc}(x, k, i)$ for $x$ all 0’s, $k$ all 1’s, and $i = 0..3$.

Hint: The Sage documentation can be found at http://www.sagemath.org/doc/reference/cryptography/sage/crypto/mq/sr.html. Our version of baby-AES corresponds to

```python
rounds = 3
rows = 2
cols = 2
exponent = 4
aes = mq.SR(rounds, rows, cols, exponents,
        allow_zero_inversions=True, star=True)
```

(b) (3 points) For later use, write a function $\text{declast}(y, k^n)$ which decrypts the last round, i.e. $\text{declast}(y, k^n)$ should return the state before entering the last round, given the ciphertext $y$ and the last round-key $k^n$. Print $\text{declast}(y, k^n)$ for $y$ all 0’s and $k^n$ all 1’s.

Hint: The inverse of MixColumns and Shiftrows are self-inverse for our baby-AES.

Hint: The inverse of an S-box is again an S-box. You can specify an S-box in Sage explicitly by

```python
mySbox = mq.SBox(14, 13, 4, 14, 3, 2, 0, 6, 15, 8,
    7, 1, 11, 9, 5, 10)
```


**Exercise 3** (the average maximal propagation ratio). (10 points)

What is the expected maximal propagation ratio for a non-trivial differential for a randomly chosen S-box ($\mathbb{F}_2^4 \to \mathbb{F}_2^4$, $\mathbb{F}_2^8 \to \mathbb{F}_2^8$, and $\mathbb{F}_2^8 \to \mathbb{F}_2^4$).

More precisely, do the following
• Randomly generate an S-box for dimensions $4 \times 4$, $8 \times 8$, and a random mapping $6 \to 4$.

• Compute the differential distribution table.

• Derive the maximal propagation ratio (for a non-trivial differential).

• Plot the distribution and mark the values for baby-AES, AES, and DES within them.