

## Cryptography Assignment 1

For the first two problems, the protocols should be simple enough to be done without a computer and, of course, without the help of a trusted outside party. They can use random coins.

1. Bob, who is color blind, goes shopping with his wife Alice. Alice finds two shirts and asks Bob which shirt Bob likes better. The shirts look identical to Bob but Alice says they look different. How can Alice convince Bob that the shirts are indeed different? (Based on a true story)
2. How do 3 office workers compute the average of their salaries without anyone revealing anything additional about their individual salaries?
3. Let  $f$  be a function that maps 128 bits to 128 bits and  $x \oplus y$  is the bitwise parity of  $x$  and  $y$ . We say  $f$  is *affine* if for all  $x, y$

$$f(x) \oplus f(y) = f(x \oplus y) \oplus f(\mathbf{0})$$

where  $\mathbf{0}$  is the 128 bit sequence of all zeros.

- (a) Show that if  $f$  and  $g$  are affine then  $h(x) = f(g(x))$  is also affine.
- (b) Show that the ShiftRow, MixColumn and RoundKey operations in the AES algorithm are all affine.
- (c) Suppose we remove all ByteSub transformations from the AES algorithm. Call this the AES- algorithm. Show that AES- computes an affine function with any key.
- (d) Show that for any  $x$  and  $y$  and keys  $k_1$  and  $k_2$  with  $f_{k_1}$  and  $f_{k_2}$  computed with the AES- algorithm,

$$f_{k_1}(x) \oplus f_{k_1}(y) = f_{k_2}(x) \oplus f_{k_2}(y).$$

- (e) Show that for the AES- algorithm if Eve has an  $x$  and  $f_k(x)$  (but not  $k$ ), Eve can quickly find  $y$  from  $f_k(y)$  for any  $y$ .

Note: The ByteSub transformation is not affine to prevent AES from being affine and having this line of attack.