CS 655 Fall, 2017, Homework 3

Due: Tuesday, November 28, 2017

1. Consider a block cipher BES, which is exactly like AES except that it omits the round function `ByteSub` from all rounds. Assume a 128-bit key is used. The last round has no `MixColumn`. Try to break BES via the Square attack. Tell how to break a four-round version of BES. How many more rounds can you break using the Square attack as presented in class? Can you break the full ten rounds?

Do not write any computer programs to solve this problem. If you feel the need to run a program, tell what the program would do, roughly how long it would run and what results you would expect from it.

2. Consider a block cipher SES, which is exactly like AES except that it omits the round function `ShiftRow` from all rounds. Assume a 128-bit key is used. The last round has no `MixColumn`. Try to break SES via the Square attack. Tell how to break a four-round version of SES. How many more rounds can you break using the Square attack as presented in class? Can you break the full ten rounds?

Do not write any computer programs to solve this problem. If you feel the need to run a program, tell what the program would do, roughly how long it would run and what results you would expect from it.

3. Consider a block cipher MES, which is exactly like AES except that it omits the round function `MixColumn` from all rounds. Assume a 128-bit key is used. Try to break MES via the Square attack. Tell how to break a four-round version of MES. How many more rounds can you break using the Square attack as presented in class? Can you break the full ten rounds?

Do not write any computer programs to solve this problem. If you feel the need to run a program, tell what the program would do, roughly how long it would run and what results you would expect from it.

4. Consider a hash function SHU with the same architecture as SHA-0. However, SHU uses XOR (of five 32-bit words) in place of the ADD (add modulo 2^{32}) operation and all 80 non-linear functions are MAJ, the majority function. SHU is similar to SHA-0 in all other respects. Tell how to find a collision in SHU if you can choose all 80 message blocks $W^{(i)}$ independently. Your solution should hash substantially fewer than 2^{80} messages.

Do not write any computer programs to solve this problem. If you feel the need to run a program, tell what the program would do, roughly how long it would run and what results you would expect from it.