The University of North Carolina at Greensboro
CSC 580: Cryptography and Security in Computing
Prof. Stephen R. Tate

Handout 9
February 2, 2017

Homework 4 – Due Tuesday, February 14

1. The Java Cryptography Architecture (JCA) is described as a "provider-based architecture." In your own words, what does this mean?

2. The AES handout mentions that there is an attack on a block cipher that requires building a table whose size is a function of the block size (see the "Block Size" discussion in the "Background" section). How much memory/storage would this require for a block cipher with 80-bit blocks?

3. Fill in the following table giving the basic parameters of AES:

Algorithm	Block Size(s)	Key Size(s)
AES		

   Imagine that we could make a special-purpose machine that could do a brute-force attack on an 80-bit key that would take, on average, 1 second to find a key in a known plaintext attack. Assuming that it could test keys for any algorithm at the same speed, approximate how long would it take, on average, to break AES with its smallest supported key? (For your answer, give a precise amount, but then give an "understandable" amount — is it a few seconds? an hour? a day? week? etc.)

   What if someone made a mistake in implementing AES, so that two bits out of every key byte were fixed and known to the attacker (for example, the first two bits of every ASCII letter are `01`) — how fast could this machine break the key in this case?