

## CS 344 Assignment 5 OTP Test List

The following table lists the various tests that are executed by p5testscript, along with the points corresponding to each of the tests.

Item	Points	Comments
keygen 20 > key20	5	key20 must exist
wc -m key20	5	Number of characters must be 21
keygen 70000 > key70000	5	Number of characters in key70000, should be 70001
enc_client plaintext1 key20 \$encport	10	Should return error about too-short key
enc_client plaintext1 key70000 \$encport	20	Should return encrypted version of plaintext1
enc_client plaintext1 key70000 \$encport > ciphertext1	10	ciphertext1 must exist
wc -m plaintext1 wc -m ciphertext1	10	Both must have same number of chars
cat ciphertext1	5	ciphertext1 should look encrypted
dec_client ciphertext1 key70000 \$encport	5	Should fail giving error that dec_client cannot use enc_server
cat plaintext1 dec_client ciphertext1 key70000 \$decport	20	Should return decrypted ciphertext1 that matches source
dec_client ciphertext1 key70000 \$decport > plaintext1_a	10	plaintext1_a must exist
cmp plaintext1 plaintext1_a	5	plaintext1 must be the same as plaintext1_a
enc_client plaintext1 key70000 \$encport > ciphertext1 & enc_client plaintext2 key70000 \$encport > ciphertext2 & enc_client plaintext3 key70000 \$encport > ciphertext3 & enc_client plaintext4 key70000 \$encport > ciphertext4 & enc_client plaintext5 key70000 \$encport > ciphertext5 & sleep 10	20	Concurrent test of encryption - look for 4 properly-sized ciphertext# files, or 5 where the 5th is 0 bytes
Should be only one error about plaintext5 being bad	5	
dec_client ciphertext1 key70000 \$decport > plaintext1_a & dec_client ciphertext2 key70000 \$decport > plaintext2_a &	15	Concurrent test of decryption - look for 4 plaintext#_a files that match the plaintext# files

---

<pre>dec_client ciphertext3 key70000 \$decport &gt; plaintext3_a &amp; dec_client ciphertext4 key70000 \$decport &gt; plaintext4_a &amp;  sleep 10  ls -pla</pre>		<p>Ten second sleep, your program must complete in this time</p>
---	--	--