Assignment 2 Testing and User Guide

Isaac Morneau; A00958405

User Guide 3

Testing 4

User Guide

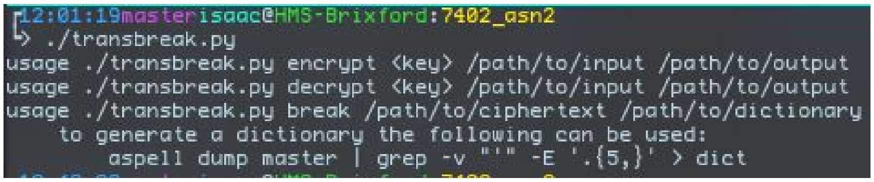
The different modes of operations are listed as follows:

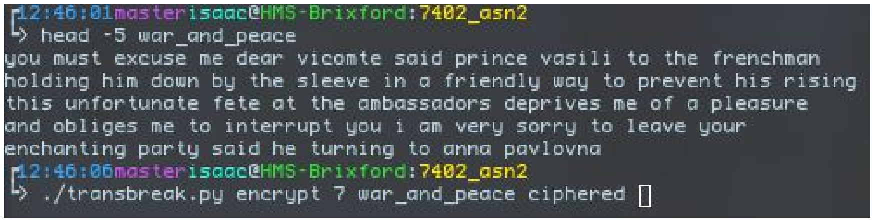
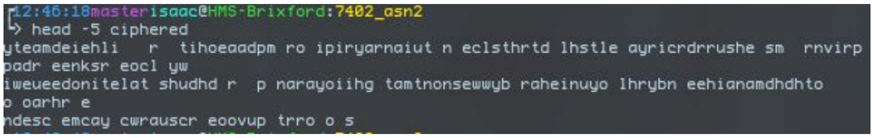
```
usage ./transbreak.py encrypt <key> /path/to/input /path/to/output
usage ./transbreak.py decrypt <key> /path/to/input /path/to/output
usage ./transbreak.py break /path/to/ciphertext /path/to/dictionary
    to generate a dictionary the following can be used:
        aspell dump master | grep -v "'" -E '.{5,}' > dict
```

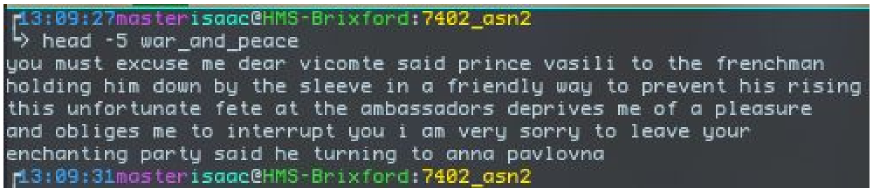
To get the help message run the script with no arguments

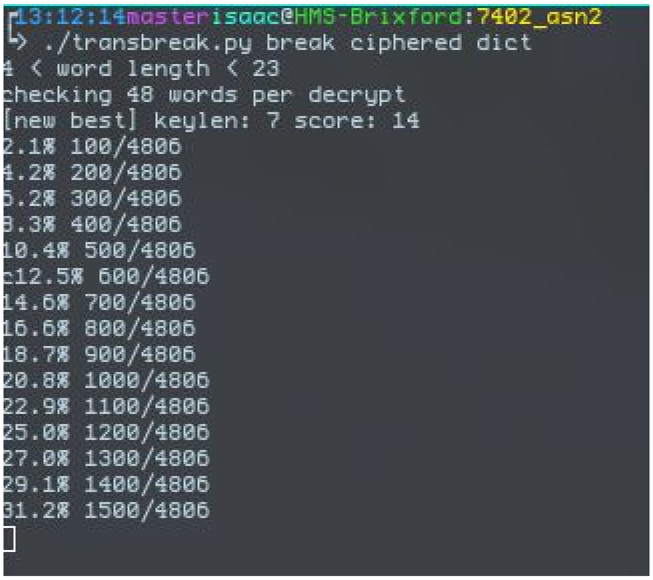
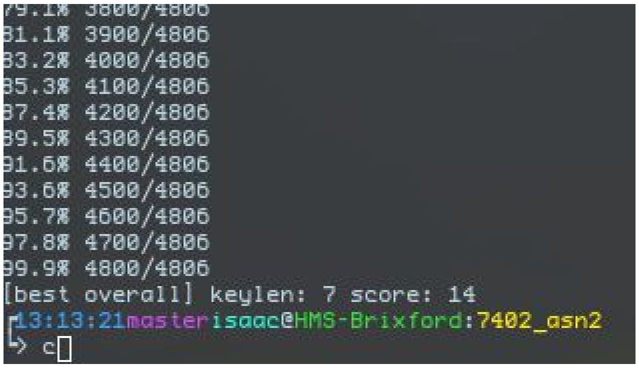
Testing

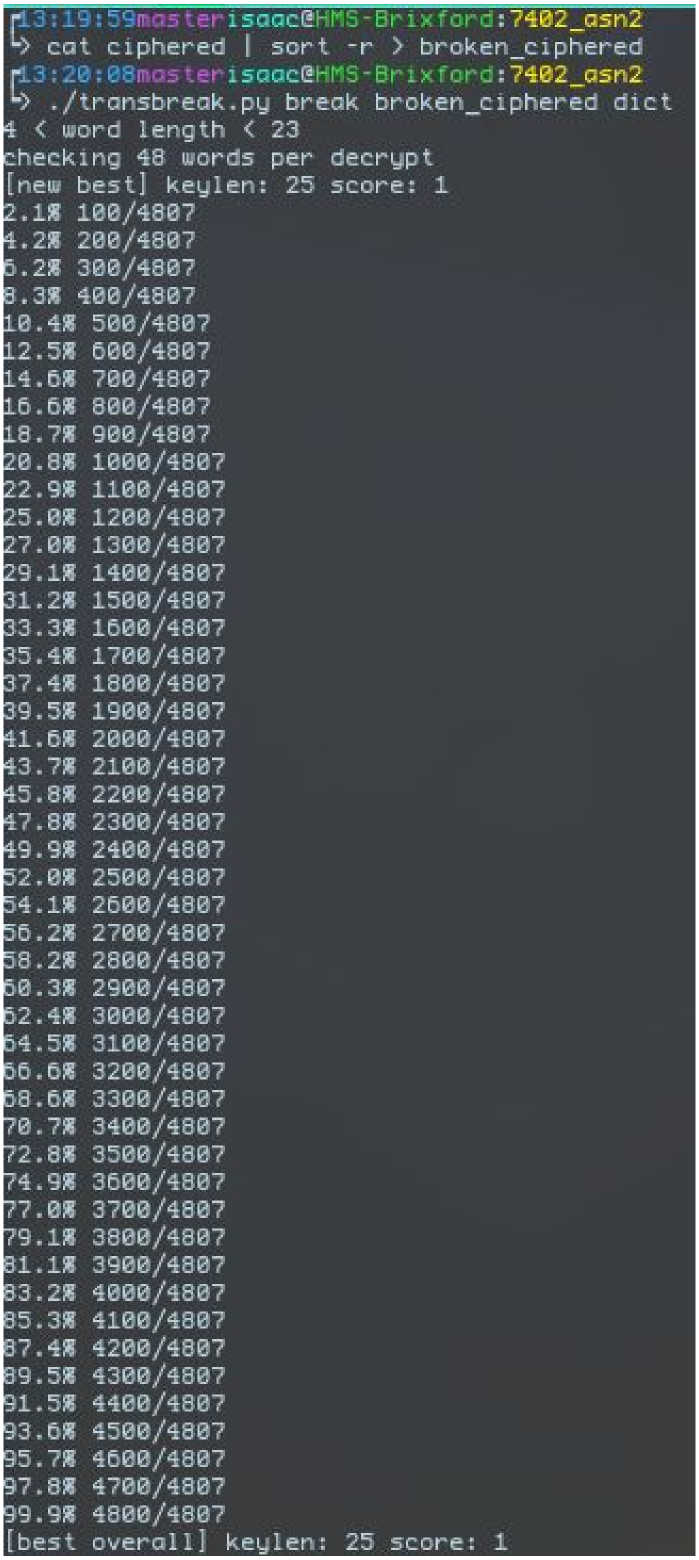
Test Case	Steps	Result

Print Usage	Run the script	
		`┌12:01:19masterisaac@HMS-Brixford:7402_asn2`
		`└> ./transbreak.py`
		`usage ./transbreak.py encrypt <key> /path/to/input /path/to/output`
		`usage ./transbreak.py decrypt <key> /path/to/input /path/to/output`
		`usage ./transbreak.py break /path/to/ciphertext /path/to/dictionary`
		`    to generate a dictionary the following can be used:`
		`        aspell dump master | grep -v "'" -E '.{5,}' > dict`
		Usage info is printed

Generate the ciphered text	Run the script as follows:
	./transbreak.py encrypt 7 war_and_peace ciphered
		
		`┌12:46:01masterisaac@HMS-Brixford:7402_asn2`
		`└> head -5 war_and_peace`
		`you must excuse me dear vicomte said prince vasili to the frenchman`
		`holding him down by the sleeve in a friendly way to prevent his rising`
		`this unfortunate fete at the ambassadors deprives me of a pleasure`
		`and obliges me to interrupt you i am very sorry to leave your`
		`enchanting party said he turning to anna pavlovna`
		`┌12:46:06masterisaac@HMS-Brixford:7402_asn2`
		`└> ./transbreak.py encrypt 7 war_and_peace ciphered ▯`
		The ciphered text is outputted
		
		`┌12:46:18masterisaac@HMS-Brixford:7402_asn2`
		`└> head -5 ciphered`
		`yteamdeiehli   r  tihoeaadpm ro ipiryarnaiut n eclsthrtd lhstle ayricrdrrushe sm  rnvirp`
		`padr eenksr eocl yw`
		`iweueedonitelat shudhd r  p narayoiihg tamtnonsewwyb raheinuyo lhrybn eehianamdhdhto`
		`o oarhr e`
		`ndesc emcay cwrauscr eoovup trro o s`

Decrypt the ciphered text	Run the script as follows:
	./transbreak.py decrypt 7 ciphered war_and_peace
		
		`┌13:09:27masterisaac@HMS-Brixford:7402_asn2`
		`└> head -5 war_and_peace`
		`you must excuse me dear vicomte said prince vasili to the frenchman`
		`holding him down by the sleeve in a friendly way to prevent his rising`
		`this unfortunate fete at the ambassadors deprives me of a pleasure`
		`and obliges me to interrupt you i am very sorry to leave your`
		`enchanting party said he turning to anna pavlovna`
		`┌13:09:31masterisaac@HMS-Brixford:7402_asn2`
		The original is recovered

Break the ciphered text	Run the script as follows: ./transbreak.py break ciphered dict	 ┌13:12:14masterisaac@HMS-Brixford:7402_asn2 └> ./transbreak.py break ciphered dict 4 < word length < 23 hecking 48 words per decrypt [new best] keylen: 7 score: 14 2.1% 100/4806 4.2% 200/4806 6.2% 300/4806 8.3% 400/4806 10.4% 500/4806 c12.5% 600/4806 14.6% 700/4806 16.6% 800/4806 18.7% 900/4806 20.8% 1000/4806 22.9% 1100/4806 25.0% 1200/4806 27.0% 1300/4806 29.1% 1400/4806 31.2% 1500/4806 Incremental progress is reported  79.1% 3800/4806 81.1% 3900/4806 83.2% 4000/4806 85.3% 4100/4806 87.4% 4200/4806 89.5% 4300/4806 91.6% 4400/4806 93.6% 4500/4806 95.7% 4600/4806 97.8% 4700/4806 99.9% 4800/4806 [best overall] keylen: 7 score: 14 ┌13:13:21masterisaac@HMS-Brixford:7402_asn2 └> c Upon completion the best key length found is reported which as we saw is the length it was encrypted with

Breaking false data	Shuffle the other cipher text or generate random ascii
	
	Run the script as follows:
	
	./transbreak.py break broken_ciphered dict
		
		`┌13:19:59masterisaac@HMS-Brixford:7402_asn2`
		`└> cat ciphered | sort -r > broken_ciphered`
		`┌13:20:08masterisaac@HMS-Brixford:7402_asn2`
		`└> ./transbreak.py break broken_ciphered dict`
		`4 < word length < 23`
		`checking 48 words per decrypt`
		`[new best] keylen: 25 score: 1`
		`2.1% 100/4807`
		`4.2% 200/4807`
		`6.2% 300/4807`
		`8.3% 400/4807`
		`10.4% 500/4807`
		`12.5% 600/4807`
		`14.6% 700/4807`
		`16.6% 800/4807`
		`18.7% 900/4807`
		`20.8% 1000/4807`
		`22.9% 1100/4807`
		`25.0% 1200/4807`
		`27.0% 1300/4807`
		`29.1% 1400/4807`
		`31.2% 1500/4807`
		`33.3% 1600/4807`
		`35.4% 1700/4807`
		`37.4% 1800/4807`
		`39.5% 1900/4807`
		`41.6% 2000/4807`
		`43.7% 2100/4807`
		`45.8% 2200/4807`
		`47.8% 2300/4807`
		`49.9% 2400/4807`
		`52.0% 2500/4807`
		`54.1% 2600/4807`
		`56.2% 2700/4807`
		`58.2% 2800/4807`
		`60.3% 2900/4807`
		`62.4% 3000/4807`
		`64.5% 3100/4807`
		`66.6% 3200/4807`
		`68.6% 3300/4807`
		`70.7% 3400/4807`
		`72.8% 3500/4807`
		`74.9% 3600/4807`
		`77.0% 3700/4807`
		`79.1% 3800/4807`
		`81.1% 3900/4807`
		`83.2% 4000/4807`
		`85.3% 4100/4807`
		`87.4% 4200/4807`
		`89.5% 4300/4807`
		`91.5% 4400/4807`
		`93.6% 4500/4807`
		`95.7% 4600/4807`
		`97.8% 4700/4807`
		`99.9% 4800/4807`
		`[best overall] keylen: 25 score: 1`
		The best score was only one word found with a key length of 25 which shows that it is probably not a valid cipher