
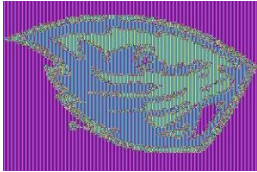
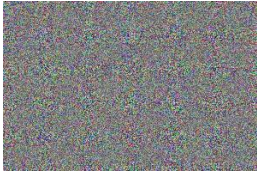

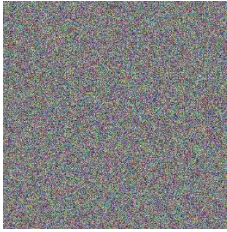
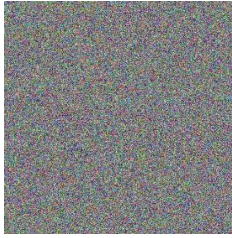


# Programming Project

## Encryption and Hashing

### 3.1 Encryption Mode – ECB vs. CBC

Original Image	Encrypted Image - ECB	Encrypted Image - CBC
		
		

For our original images we have the beaver logo that I downloaded off of the internet and a picture of a daisy that I had taken for an art project a few years ago. When we encrypt both of these images using CBC encryption, in both cases we get new heavily distorted images of what looks like white noise. However, the results of encrypting these images using ECB encryption. The beaver logo is easily made out. It remains to have 3 colors present and it only looks a little more jagged/fuzzy. The daisy image on the other hand looks just as distorted as it did in the CBC encrypted image. The lack of patterns and larger variety in colors makes it easy for ECB to do well in encrypting the image.

### 3.2 Encrypting with OpenSSL

To find the key that was used to encrypt the message “This is a top secret.”, we began encrypting the message using every word given to us in the dictionary file “words.txt”. We would then check each of these encrypted messages with the encrypted message we were given to find the key of. If at any point our encrypted message matches the given encrypted message, we stop what we are doing. We know that the key used to get the encrypted message is the same one we just used. Through this process we uncovered that the key used to encrypt our message was “median”.

### 3.3 Weak vs Strong Collision Resistance

The longest part of this problem is waiting for your results. Based on the material from class, we can predict that the weak collision resistance will take around 8,388,608 attempts to break a 24 bits (3 bytes) hash and it will take 16,777,216 attempts to break the strong collision resistance hash. These attacks each take a lengthy amount of time to enact even after shortening the length of hash. These are the results that were gathered through the tests:

TRIAL	ATTEMPTS					
	16 bits		20 bits		24 bits	
	WEAK	STRONG	WEAK	STRONG	WEAK	STRONG
1	75,272	84,072	55,264	1,189,088	3,052,170	17,135,056
2	33,786	34,505	414,823	609,600	20,698,099	5,237,872
3	10,570	15,928	267,027	227,206	24,450,460	12,534,933
4	22,952	3,133	868,418	234,306	2,325,180	8,789,389
5	14,350	99,707	1,577,376	572,856	21,224,807	11,000,700
6	54,268	130,345	426,083	69,130	2,032,956	18,191,028
7	247,007	21,704	89,911	339,823	6,400,233	46,946,614
8	25,973	7,648	218,868	2,142,887	7,304,152	22,640,628
9	21,438	115,604	282,353	803,831	1,789,023	2,046,977
10	3,593	239,522	692,571	60,821	2,286,633	43,403,737
11	75,415	28,130	3,770,094	1,684,634	13,397,035	936,264
12	3,315	7,643	14,212	513,818	22,474,545	22,579,653
13	9,217	20,300	1744,715	3,488,119	6,665,007	12,277,742
14	139,106	31,492	199,114	1,645,590	2,937,374	467,344
15	41,020	161,821	1178,046	649,605	2,055,925	2,715,195
Average	34,837	49,885	672,159	962,055	8,637,582	15,666,179

Based off the results from our tests, we can observe that weak collision resistance is easier to break using brute force than strong collision resistance. The weak collision resistance attack and the strong collision resistance attack match the way that we expected them to behave quite closely.