Simple Brute Force Attack

Examples

Steven Gordon

1 A Simple ASCII Example

Assume 7-bit ASCII is used, then the message “Hello” is, in binary:

1001000 1100101 1101100 1101100 1101111

2 Brute Force Attack

Lets assume we have an encryption algorithm which is the XOR of each *n* bit sequence with a *k* bit key. The key is repeated where necessary.

The message “Steve” can be represented in binary using an ASCII conversion

Character	*Decimal*	*Binary*
S	83	1010011
t	116	1110100
e	101	1100101
v	118	1110110

So the plaintext is:

```
P =   10100111110100110010111101101100101
```

Consider a 2-bit key, say K = 01

The corresponding ciphertext is:

```
P =   10100111110100110010111101101100101 XOR
K =   01010101010101010101010101010101010
C =   11110010100001100111101000111001111
```

If this was converted to ASCII, we would have:

Binary	*Decimal*	*Character*
1111001	121	y
0100001	33	!
1001111	79	O
0100011	35	#
1001111	79	O

If the attacker new the ciphertext only, then a brute force attack would reveal the following.

Try key k = 00 on the ciphertext C gives:

```
C =   11110010100001100111101000111001111 XOR
K =   00000000000000000000000000000000000
P =   11110010100001100111101000111001111
```

Converting to ASCII characters gives:

Binary	*Decimal*	*Character*
1111001	121	y
0100001	33	!
1001111	79	O
0100011	35	#
1001111	79	O

Try key = 10:

```
C =   11110010100001100111101000111001111 XOR
K =   10101010101010101010101010101010101
P =   01011000001011001101000010010011010
```

Binary	*Decimal*	*Character*
0101100	44	,
0001011	11	VT
0011010	26	SUB
0001001	9	TAB
0011010	26	SUB

Try key, k =11:

```
C =   11110010100001100111101000111001111 XOR
K =   11111111111111111111111111111111111
P =   00001101011110011000010111000110000
```

Binary	*Decimal*	*Character*
0000110	6	ACK
1011110	94	^
0110000	48	0
1011100	92	\
0110000	48	0

So the results of the brute force attack are:

Key	*Plaintext*	*ASCII*
00	11110010100001100111101000111001111	y!O#O
01	10100111110100110010111101101100101	Steve
10	01011000001011001101000010010011010	,[VT][SUB][TAB][SUB]
11	00001101011110011000010111000110000	[ACK]^0\0

The attacker would guess the original plaintext was “Steve”.