

Below are 7 ciphertexts, each of which was generated by encrypting some 31-character ASCII plaintext with the one-time pad using the same key (code for the encryption program used is given below). Decrypt them and recover all 7 plaintexts, each of which is a grammatically correct English sentence. Note: For this problem it is easiest to use a combination of automated analysis plus human insight and even occasional guessing. As long as you can decrypt them all, it doesn't matter how you do it.

The 7 ciphertexts are:

```
BB3A65F6F0034FA957F6A767699CE7FABA855AFB4F2B520AEAD612944A801E
BA7F24F2A35357A05CB8A16762C5A6AAAC924AE6447F0608A3D11388569A1E
A67261BBB30651BA5CF6BA297ED0E7B4E9894AA95E300247F0C0028F409A1E
A57261F5F0004BA74CF4AA2979D9A6B7AC854DA95E305203EC8515954C9D0F
BB3A70F3B91D48E84DF0AB702ECFEEB5BC8C5DA94C301E0BECDD241954C831E
A6726DE8F01A50E849EDBC6C7C9CF2B2A88E19FD423E0647ECCB04DD4C9D1E
BC7570BBBF1D46E85AF9AA6C7A9CEFA9E9825CFD5E3A0047F7CD009305A71E
```

You don't need to understand this, but if you think this helps, the above ciphers are generated using the following code.

```
#include
#define KEY_LENGTH 31

main(){
    unsigned char ch;
    FILE *fpIn, *fpOut;
    int i;
    unsigned char key[KEY_LENGTH] = {0x00, 0x00, 0x00, 0x00,
        0x00, 0x00, 0x00, 0x00,
        0x00, 0x00, 0x00, 0x00,
        0x00, 0x00, 0x00, 0x00,
        0x00, 0x00, 0x00, 0x00,
        0x00, 0x00, 0x00, 0x00,
        0x00, 0x00, 0x00, 0x00,
        0x00, 0x00, 0x00};
    // Of course, I did not use the all-0 key when generating the 7 ciphertexts above!

    fpIn = fopen("messages.txt", "r");
    fpOut = fopen("ctexts.txt", "w");

    i=0;

    while (fscanf(fpIn, "%c", &ch) != EOF) {
        fprintf(fpOut, "%02X", ch^key[i]);
        i++;
    }
```

```
    if (i==31) {  
        fprintf(fpOut, "\n");  
        i=0;  
        fscanf(fpIn, "%c", &ch);  
    }  
}  
  
fclose(fpIn);  
fclose(fpOut);  
  
return;  
}
```

Deliverables:

1. Deciphered plain-text for each of the 7 ciphertexts.
2. Description of how you solved.
3. Automation code you developed to crack the codes.