**现代密码学**

**实验一**

1. Coursera Dan Boneh Week 1 Program Assignment

Many Time Pad

1.  The secret message is: When using a stream cipher, never use the key more than once

..................................................................................C

key: 66396e89c9dbd8cc9874352acd6395102eafce78aa7fed28a07f6bc98d29c50b69b0339a19f8aa401a9c6d708f80c066c763fef0123148cdd8e802d05ba98777335daefcecd59c433a6b268b60bf4ef03c9a611098bb3e9a3161edc7b804a33522cfd202d2c68c57376edba8c2ca50027c61246ce2a12b0c4502175010c0a1ba4625786d911100797d8a47e98b0204c4ef06c867a950f11ac989dea88fd1dbf16748749ed4c6f45b384c9d96c4

Decrypt all messages using the key:

[1] We can factor the number 15 with quantum computers. We can also factor the number 15 with a dog trained to bark three times - Robert Harley

[2] Euler would probably enjoy that now his theorem becomes a corner stone of crypto - Annonymous on Euler's theorem

[3] The nice thing about Keeyloq is now we cryptographers can drive a lot of fancy cars - Dan Boneh

[4] The ciphertext produced by a weak encryption algorithm looks as good as ciphertext produced by a strong encryption algorithm - Philip Zimmermann

[5] You don't want to buy a set of car keys from a guy who specializes in stealing cars - Marc Rotenberg commenting on Clipper

[6] There are two types of cryptography - that which will keep secrets safe from your little sister, and that which will keep secrets safe from your government - Bruce Schneier

[7] There are two types of cyptography: one that allows the Government to use brute force to break the code, and one that requires the Government to use brute force to break you

[8] We can see the point where the chip is unhappy if a wrong bit is sent and consumes more power from the environment - Adi Shamir

[9] A (private-key) encryption scheme states 3 algorithms, namely a procedure for generating keys, a procedure for encrypting, and a procedure for decrypting.

[10] The Concise OxfordDictionary (2006) deï¬nes crypto as the art of writing o r solving codes.

[11] The secret message is: When using a stream cipher, never use the key more than once

1. PA1 option

Write a program that allows you to "crack" ciphertexts generated using a Vigenere-like cipher, where byte-wise XOR is used instead of addition modulo 26.

Cryptography is the practice and study of techniques for, among other things, secure communication in the presence of attackers. Cryptography has been used for hundreds, if not thousands, of years, but traditional cryptosystems were designed and evaluated in a fairly ad hoc manner. For example, the Vigenere encryption scheme was thought to be secure for decades after it was invented, but we now know, and this exercise demonstrates, that it can be broken very easily.

1. http://www.cryptopals.com/sets/1
2. Convert hex to base64

Base64 Encoded: SSdtIGtpbGxpbmcgeW91ciBicmFpbiBsaWtlIGEgcG9pc29ub3VzIG11c2hyb29t

1. Fixed XOR

XOR Result: 746865206b696420646f6e277420706c6179

1. Single-byte XOR cipher

Decrypted Text: Cooking MC's like a pound of bacon

Key: 0x58

1. Detect single-character XOR

plaintext: Now that the party is jumping

Key: 0x35

1. Implement repeating-key XOR

Encrypted: 0b3637272a2b2e63622c2e69692a23693a2a3c6324202d623d63343c2a26226324272765272a282b2f20690a652e2c652a3124333a653e2b2027630c692b20283165286326302e27282f

1. Break repeating-key XOR

keysize: 29

message: I'm back and I'm ringin' the bell

A rockin' on the mike while the fly girls yell

In ecstasy in the back of me

Well that's my DJ Deshay cuttin' all them Z's

Hittin' hard and the girlies goin' crazy

Vanilla's on the mike, man I'm not lazy.

I'm lettin' my drug kick in

It controls my mouth and I begin

To just let it flow, let my concepts go

My posse's to the side yellin', Go Vanilla Go!

Smooth 'cause that's the way I will be

And if you don't give a damn, then

Why you starin' at me

So get off 'cause I control the stage

There's no dissin' allowed

I'm in my own phase

The girlies sa y they love me and that is ok

And I can dance better than any kid n' play

Stage 2 -- Yea the one ya' wanna listen to

It's off my head so let the beat play through

So I can funk it up and make it sound good

1-2-3 Yo -- Knock on some wood

For good luck, I like my rhymes atrocious

Supercalafragilisticexpialidocious

I'm an effect and that you can bet

I can take a fly girl and make her wet.

I'm like Samson -- Samson to Delilah

There's no denyin', You can try to hang

But you'll keep tryin' to get my style

Over and over, practice makes perfect

But not if you're a loafer.

You'll get nowhere, no place, no time, no girls

Soon -- Oh my God, homebody, you probably eat

Spaghetti with a spoon! Come on and say it!

VIP. Vanilla Ice yep, yep, I'm comin' hard like a rhino

Intoxicating so you stagger like a wino

So punks stop trying and girl stop cryin'

Vanilla Ice is sellin' and you people are buyin'

'Cause why the freaks are jockin' like Crazy Glue

Movin' and groovin' trying to sing along

All through the ghetto groovin' this here song

Now you're amazed by the VIP posse.

Steppin' so hard like a German Nazi

Startled by the bases hittin' ground

There's no trippin' on mine, I'm just gettin' down

Sparkamatic, I'm hangin' tight like a fanatic

You trapped me once and I thought that

You might have it

So step down and lend me your ear

'89 in my time! You, '90 is my year.

You're weakenin' fast, YO! and I can tell it

Your body's gettin' hot, so, so I can smell it

So don't be mad and don't be sad

'Cause the lyrics belong to ICE, You can call me Dad

You're pitchin' a fit, so step back and endure

Let the witch doctor, Ice, do the dance to cure

So come up close and don't be square

You wanna battle me -- Anytime, anywhere

You thought that I was weak, Boy, you're dead wrong

So come on, everybody and sing this song

Say -- Play that funky music Say, go white boy, go white boy go

play that funky music Go white boy, go white boy, go

Lay down and boogie and play that funky music till you die.

Play that funky music Come on, Come on, let me hear

Play that funky music white boy you say it, say it

Play that funky music A little louder now

Play that funky music, white boy Come on, Come on, Come on

Play that funky music

key: Terminator X: Bring the noise

1. MTC3 Cracking SHA1-Hashed Passwords

<https://www.mysterytwisterc3.org/en/challenges/level-2/cracking-sha1-hashed-passwords>

ans: (Q=win\*5

t: 2 seconds