**现代密码学**

**实验二**

1. MTC3 AES key — encoded in the machine readable zone of a European ePassport <https://www.mysterytwisterc3.org/en/challenges/level-2/aes-key--encoded-in-the-machine-readable-zone-of-a-european-epassport>

Key: ea8645d97ff725a898942aa280c43179

Decrypted message: Herzlichen Glueckwunsch. Sie haben die Nuss geknackt. Das Codewort lautet: Kryptographie!

1. http://www.cryptopals.com/sets/2
2. Implement PKCS#7 padding

Padded text: b'hello, world!\x07\x07\x07\x07\x07\x07\x07'

Unpadded text: b'hello, world!'

1. Implement CBC mode

plaintext: 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

1. An ECB/CBC detection oracle
2. Byte-at-a-time ECB decryption (Simple)

Plaintext:

Rollin' in my 5.0

With my rag-top down so my hair can blow

The girlies on standby waving just to say hi

Did you stop? No, I just drove by

1. ECB cut-and-paste

{'foo': 'bar', 'baz': 'qux', 'zap': 'zazzle'}

email=foo@bar.com&uid=10&role=user

email=foo@bar.com&uid=10&role=user

{'email': 'foo@bar.com', 'uid': '10', 'role': 'usmadmi'}

1. Byte-at-a-time ECB decryption (Harder)

Block Size is 16

Mode of encryption is ECB

Calculated Length of Prefix = 0

Possible end of plaintext: No matches found.

Plaintext:

Rollin' in my 5.0

With my rag-top down so my hair can blow

The girlies on standby waving just to say hi

Did you stop? No, I just drove by

1. PKCS#7 padding validation

ICE ICE BABY

Invalid PKCS#7 padding

Invalid PKCS#7 padding

1. CBC bit flipping attacks

Plaintext: b'comment1=cooking%20MCs;userdata=AAAAAAAAAAAAAAAA;comment2=%20like%20a%20pound%20of%20bacon'

Ciphertext: b'\x0cGM:\x85q:G\xf2f\x98\xe0\xb1 \x9a\xfbBK\x13\xc4\xaf\xac6w\xa3\x98\xe6H\xabc:\xe2\xad~\xd9\x84\xd9\xe5\xa2\\\xe3\*\xdd\x179[\xd5AJ}\xb98\xf5\x01\xb9\x81r\xab\xda\xbf}cvx\x99\xbe\xd6\rX0\xbc\x84\xc4g\x84n\xd2\x8c\xf9K\xcb\x8c\x99a\xf0rc\x0c\xbc\xda\xd5\x9dF\x83+\x97'

Decrypted: b'comment1=cooking\xff\xb7F`\xb9C\x86\x108\xfa\x8f~\xd6\xd2\xe5\x9f;admin=true;AAAA;comment2=%20like%20a%20pound%20of%20bacon'

Bitflipping attack successful: True