دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکدهٔ مهندسی کامپیوتر و فنآوری اطلاعات

مبانی امنیت اطلاعات

(ترم بهمن ۹۸)

Cipher Modes

نستوه طاهری جوان

nastooh@aut.ac.ir

حالت های رمزهای بلاکی

- ✓ نکتهٔ مهم در همهٔ الگوریتم های رمزنگاری بلوکی (چه متقارن، چه نا متقارن)

بلوک های دادهٔ یکسان، همواره خروجی رمزشدهٔ مشابه دارند!

سوال:

آیا این مساله اهمیتی دارد؟

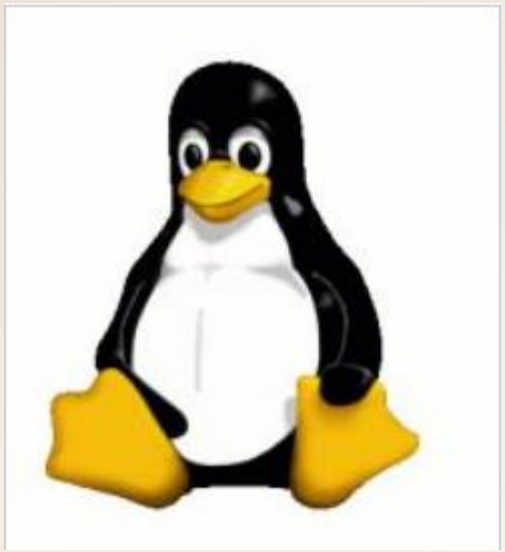
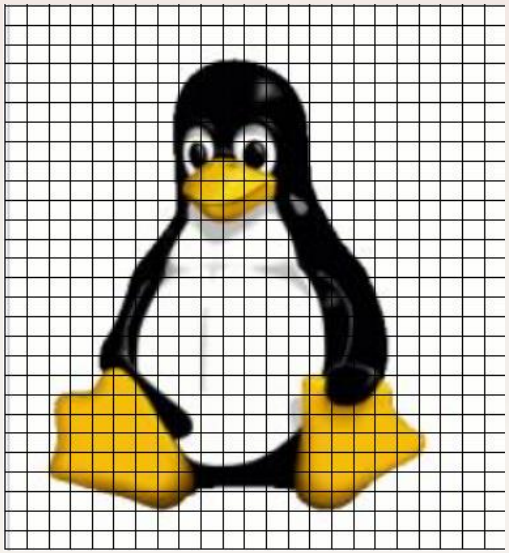
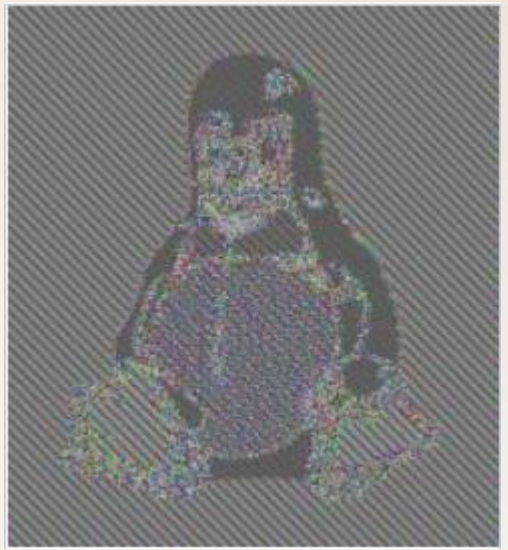
مرجع

Cryptography and Network Security, William Stallings, 7th ed.,
Sections 7.2 to 7.6.

nastooh@aut.ac.ir

حالت های رمزهای بلاکی

- ✓ مثال:

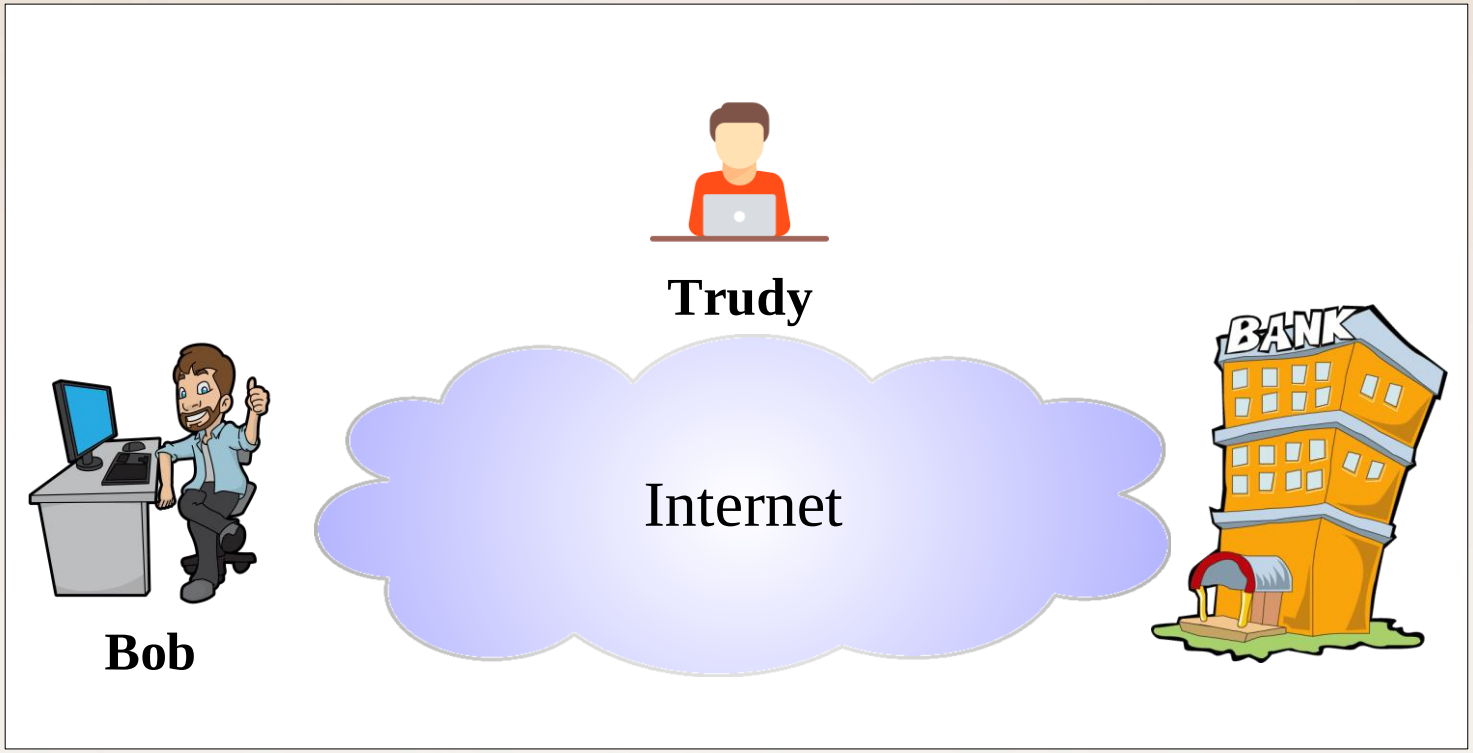
شکل برای توضیح شفاهی

nastooh@aut.ac.ir

حالت های رمزهای بلاکی

- مثال:

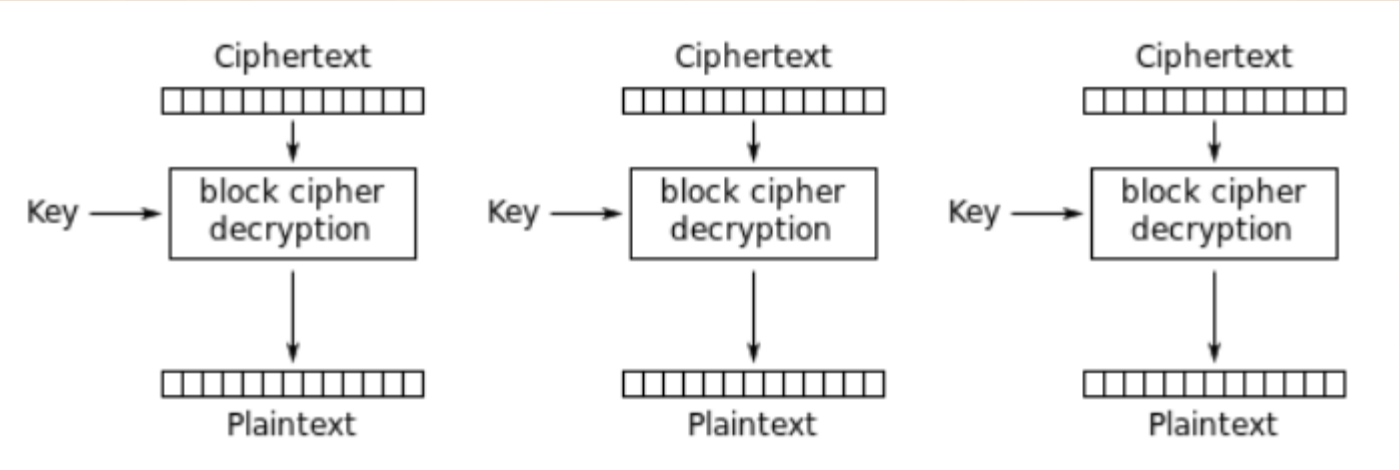
ارسال پسورد رمز شده برای بانک!!!



شکل برای توضیح شفاهی

ECB Mode

✓ حالت ECB (Electronic Code Book)



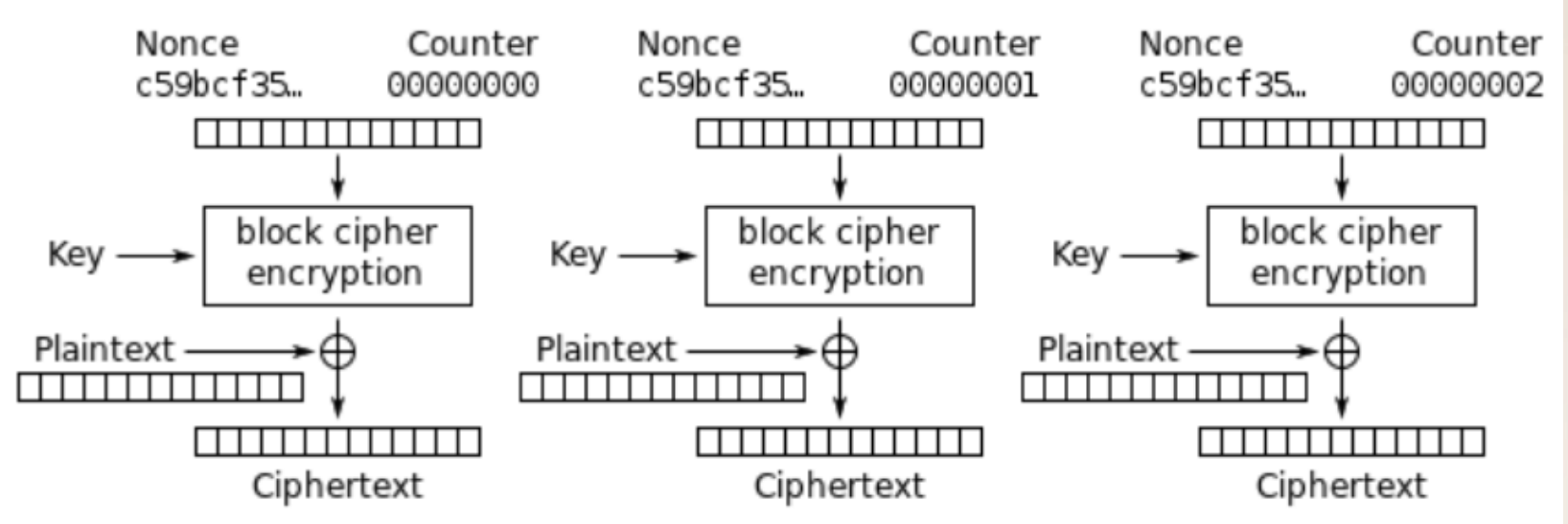
مزیت: سادگی

عیب: آشکار بودن الگوی کلی داده ها

nastooh@aut.ac.ir

CTR Mode

✓ حالت CTR (Counter)

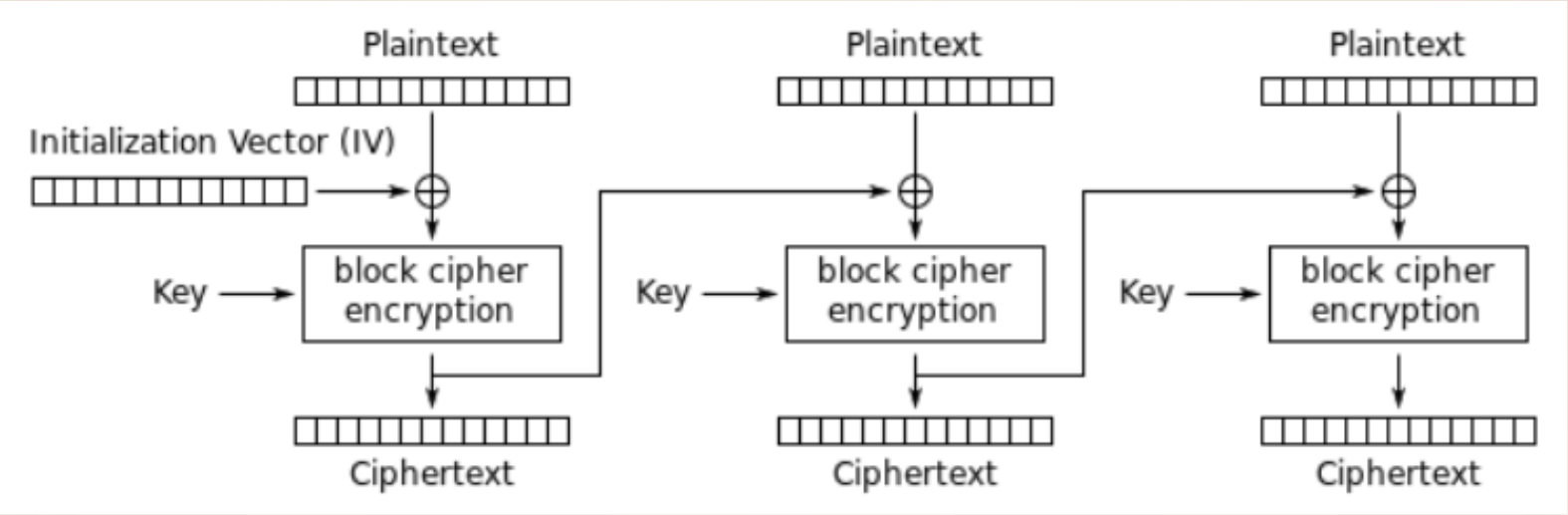


- می توان این روش را نوعی One-Time-Pad در نظر گرفت.
  - عملیات مرحلهٔ رمزنگاری در هر گام، در واقع یک کلید یکتا برای XOR ایجاد میکند.
  - ورودی رمزگذاری دو بخش دارد، بخش ثابت (و تصادفی) و بخش شمارنده

nastooh@aut.ac.ir

CBC Mode

✓ حالت CBC (Cipher Block Chaining)



بالتبع رمزگشایی هم با عکس این الگو انجام خواهد شد.

مزیت: هر قطعه به تمام قطعه های پیشین وابسته است.

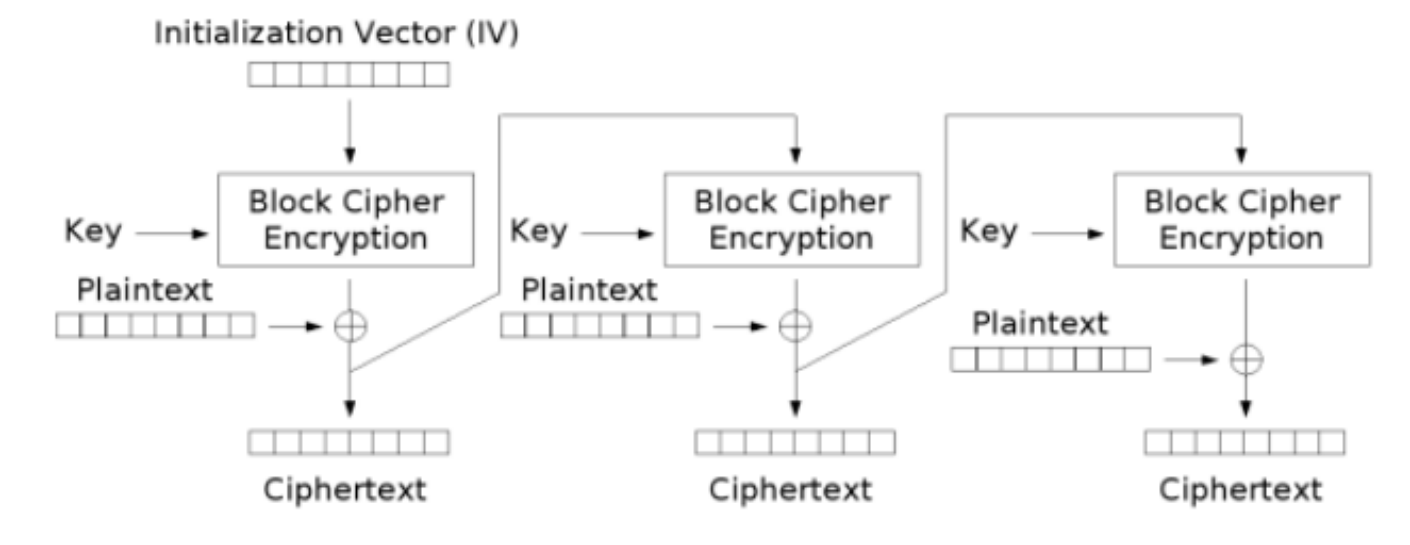
- در هم ریخته شدن الگوی داده اصلی در داده رمز شده

عیب: عدم امکان موازی سازی محاسبات در رمزگذاری (در رمزگشایی چه؟)

nastooh@aut.ac.ir

CFB Mode

✓ حالت CFB (Cipher Feedback)



- این روش، به نوعی معکوس روش CBC است.
- می توان این روش را نوعی One-Time-Pad در نظر گرفت.
  - عملیات مرحلهٔ رمزنگاری در هر گام، در واقع یک کلید یکتا برای XOR ایجاد میکند.
- دربارهٔ شباهت و ارتباط این شیوه با رمزنگاری جریانی تفکر کنید.

nastooh@aut.ac.ir

حالت های رمز

- در هر یک از حالت های رمز، میتوان به فراخور از الگوریتم رمزنگاری متفاوتی استفاده کرد.
- به مسالهٔ انتشار خطاهای رسانهٔ انتقال، حین عملیات رمزگشایی در روش های مختلف دقت کنید.
  - هم به میزان تاثیرِ مخرب خطاهای رسانه انتقالِ دادهٔ رمز شده و هم به تغییرات عمدی ترودی، هنگام مبادلهٔ دادهٔ رمز شده.
- حالت های رمز دیگری نیز وجود دارند، مانند:
  - Propagating cipher block chaining (PCBC)
  - Output feedback (OFB)

  که تغییریافتهٔ حالت های پیشین هستند.

nastooh@aut.ac.ir

منابع

[1] William Stallings, “Cryptography and Network Security,” 7th ed.

nastooh@aut.ac.ir

پایان

nastooh@aut.ac.ir