«به نام خدا»

تمرین اول درس مبانی امنیت
امیرمحمد پیرحسنلو
9531414

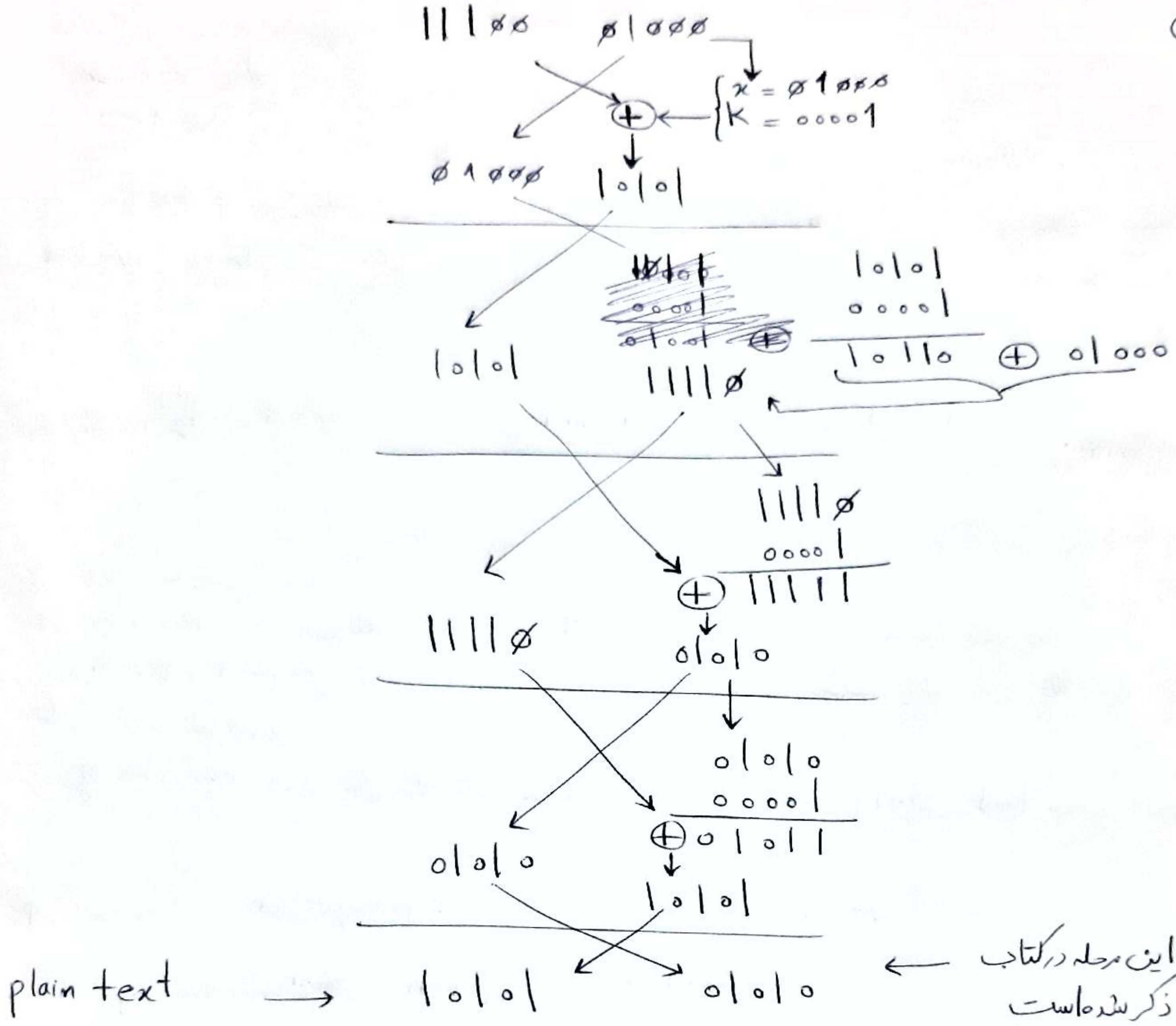
① Threat : عامل بالقوه برای نقض امنیت مثلاً عدم رمز کردن پسورد کاربران یک سایت در پایگاه داده
Attack : اقدام عملی برای نقض امنیت برای مثال اقدام برای غیرفعال سازی سرویس یک سایت .

② الف) confidentiality ب) availability ج) integrity د) availability

③ سایت سنجش
الف) integrity ← رتبه ی کنکور دانشجویان و دانش آموزان نباید به صورت غیرمجاز تغییر کند.
ب) confidentiality ← رتبه ی کنکور هر فرد تنها توسط آن فرد قابل مشاهده باشد و این اطلاعات برای سایر افراد افشا نشود.
ج) availability ← در زمان اعلام نتایج سایت همواره سرویس دهد و با افزایش load سرویس متوقف نشود.

④ الف) masquerade : ورود به gmail افراد با دسترسی به رمز عبور آن ها
مکانیزم : استفاده از 2 step verification (prevention)
ب) حملات با overhead و load بالا روی سرورهای بانک یا سازمان ها (dos)
مکانیزم : prevention
استفاده از firewall ها و ساخت شبکه با معماری distributed و ایجاد سرور آماده به کار به ازای هر سرور

ج) Replay : برای مثال text dependent speaker verification
مکانیزم : prevention
فرستنده و گیرنده یک sessionkey کاملاً تصادفی تولید کنند که تنها برای یک transaction معتبر است.

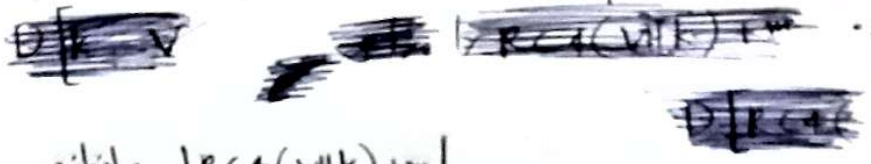

111ØØ
Ø1ØØØ
x = Ø1ØØØ
K = 00001
Ø1ØØØ
10101
10101
00001
10110
01000
10101
1111Ø
1111Ø
00001
11111
1111Ø
01010
01010
00001
01011
01010
10101
plain text
10101
01010
این مرحله در کتاب
ذکر شده است

$keylen = L_k$

$T = V$

$|T| = L_V$

ابتدا L_V بیت اول پیام دریافتی را دور می‌ریزد. حال $RC4(V||k)+m$ می‌ماند.



k' ← رمز تولید شده توسط keystream generator

$|RC4(V||k)+m|$ ← اندازه

2 است:

② برای تمام حالات m که تعدادشان برابر

① $M = (RC4(V||k)+m) - m'$ که m' یکی از حالات بالا است را حساب کن.

② $N = D[M, K]$ را محاسبه کن. ← کلید مشترک

③ L_V بیت اول N را دور بریز و حاصل را در U قرار بده.

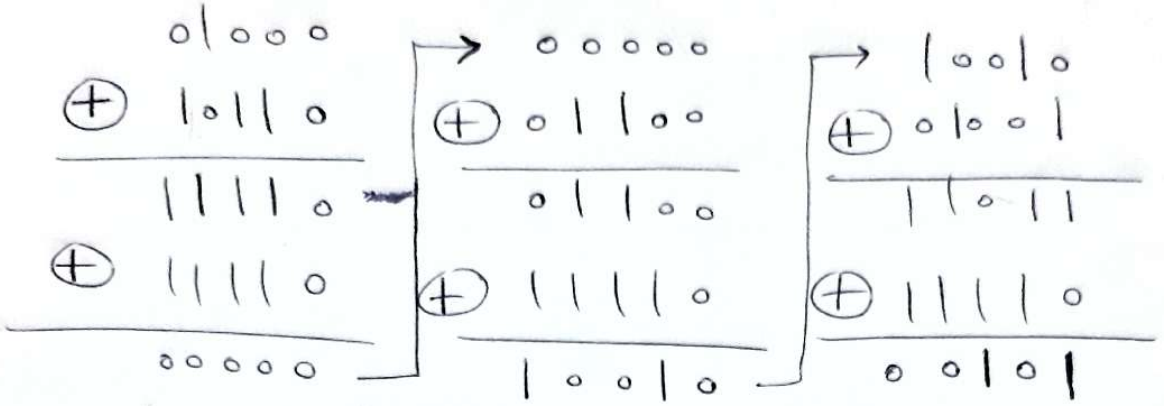
④ اگر $k = U$ نشد، m' متن اصلی است، در غیر این صورت برو به مرحله‌ی ② و یک m' جدید انتخاب کن.

(الف ⑦

ECB:

	01000	01100	01001
⊕	11110	11110	11110
	10110	10010	10111 ← cipher text

CBC:



cipher text ⟶ 00000 10010 00101

ب)

(A) hardware efficiency: اجرای موازی رمزگشایی روی blockهای رمزشده

(B) software efficiency:

به علت قابلیت اجرای موازی، بهره وری پردازنده هایی که از قابلیت اجرای موازی بهره می برند مانند SIMD ها بالا رفته است.

(C) preprocessing: می توان پیش پردازش را مستقل از ورودی plaintext یا ciphertext انجام داد.

(d) random access: هر بلاکی را می توانیم زودتر پردازش کنیم.

(e) provable security: حداقل به اندازه ی سایر الگوریتم ها امن است.

(f) simplicity: تنها پیاده سازی بخش رمزگذاری لازم است.