

\* Security mode ← از RAN به کاربر  
Command

له انتخاب الوریتم

له تأمین integrity ✓

له encryption ✗

\* کاربر فرستادن قابلیت ها  
سرور Core انتخاب قابلیت

\* Attacker فرستادن قابلیت ها را خراب نمی کند؟

له علاء بکریه فقط الوریتم صفر را میبرد می کند

له جواب Core را با قابلیت های فرستاده حد کنیم

له آرتیفات بود به جمله صورت گرفته

\* در شل ۲ به حد اقل برای الوریتم انتخاب کنیم

له فقط صفر؟ به جمله گر

$$C_k \leftarrow P_k$$

cipher text

key stream (دوره ستاد پزیری داشته باشد)

count - c در این موقع دخیل است