تکلیف سری سوم مبانی رمزنگاری

---

۱. با فرض دانستن plaintext ، یک حمله بر روی رمزهای بلوکی به صورت جستجوی کامل فضای کلید (Exhaustive key search) انجام می‌شود که در آن طول کلید k بیت و طول بلوک برابر با n است. (n > k)

۱-۱. چند جفت plaintext و ciphertext برای شکستن موفق یک رمز بلوکی در مد ECB مورد نیاز است؟ در بدترین حالت چه تعداد کلید باید مورد بررسی قرار گیرد؟

۱-۲. فرض کنید که بردار اولیه (IV) در رمز بلوکی در مد CBC آشکار شده‌است. چند جفت plaintext و ciphertext برای انجام یک حمله به صورت جستجوی کامل فضای کلید مورد نیاز است؟ در بیشترین حالت چه تعداد کلید باید بررسی شوند؟

۱-۳. هنگامی که بردار اولیه (IV) را نمی دانیم، چند جفت plaintext و ciphertext مورد نیاز است؟

۱-۴. آیا شکستن یک رمز بلوکی در مد CBC با جستجوی کامل فضای کلید نسبت به شکستن یک رمز بلوکی در مد ECB سخت تر است؟

۲. مخفی کردن بردار اولیه (IV) در مد OFB ، جستجوی کامل فضای کلید را پیچیده تر نمی‌کند. توضیح دهید چگونه می‌توان یک حمله Brute-force attack با یک IV ناشناخته انجام داد؟

۳. تمامی چند جمله های تحویل ناپذیر (irreducible polynomial) روی میدان GF(2) بیابید.

۴. رمز AES با طول بلوک ورودی 128 بیت و طول کلید 128 بیت در نظر بگیرید. اگر همه‌ی بیت‌های متن اصلی (plaintext) برابر با ’1‘ باشد و اولین زیر کلید دارای 128 بیت ’1‘ باشد، خروجی دور اول را تعیین کنید.

تمرین کریپتول

Search about one of the below topics of your choice and write a text with at least 500 words about this topic.

- • Differences between stream and block ciphers
- • PRESENT block cipher
- • Brute-force attack

5. Encrypt your text using the AES algorithm and your desired key.