«به نام خدا»

تکلیف سوم – مرضیه علیدادی – 9631983

1.

1.1.

Operation mode	Description	Data Unit Size
ECB	متن اصلی را تکه تکه می کند به قالب های n بیتی. سپس متن n بیتی را با کلید n بیتی رمز می کند و متن رمز شده ی n بیتی را حاصل می شود.	n بیت
CBC	در مرحله ی اول، متن m بیتی را با یک initial vector، XOR می کند. متن m بیتی حاصل را با کلید m بیتی رمز می کند و متن رمز شده ی m بیتی را حاصل می شود. در مراحل بعدی، به همین شکل تکرار می شود. ولی به جای استفاده از initial vector، از متن رمز شده ی قالب قبلی استفاده می کند.	m بیت
CFB	در مرحله ی اول Initial vector را با کلید رمز می کند. یک key stream حاصل می شود. این KS ای که r بیت است را با حداکثر r بیت از متن اصلی XOR می کند. و یک متن رمز شده به اندازه ی متن رمز شده حاصل می شود. در مراحل بعدی، به همین شکل تکرار می شود. ولی به جای استفاده از initial vector، از متن رمز شده ی قالب قبلی استفاده می کند.	r بیت
OFB	در مرحله ی اول Initial vector را با کلید رمز می کند. یک key stream حاصل می شود. این KS ای که b بیت است را با حداکثر b بیت از متن اصلی XOR می کند. و یک متن رمز شده به اندازه ی متن رمز شده حاصل می شود. در مراحل بعدی، به همین شکل تکرار می شود. ولی به جای استفاده از initial vector، از KS قالب قبلی استفاده می کند.	b بیت
CTR	Initial vector و counter value را با c بیت کلید رمز می کند. یک key stream حاصل می شود. این KS ای که c بیت است را با c بیت متن اصلی XOR می کند. و یک متن رمز شده ی c بیتی حاصل می شود.	c بیت

1.2.

متن اصلی های مشخص، متن های رمز شده ی مشخصی را برای ما تولید می کنند. بنابراین اگر یک پیامی دوبار ارسال شود، به راحتی قابل تشخیص است که این دو پیام با هم یکسان بوده اند. هر بلاک از قبلی مستقل است و می توان از این قضیه سو استفاده کرد. یک بیت از یک بلاک اگر خراب شود، بسته به الگوریتم رمز، بخش قابل توجهی از آن بلاک خراب می شود.

---

2. A missing or deleted bit in y_i affects the i-th feedback bit which enters the shift register of size of κ bit. After κ + 1 steps, the affected feedback bit leaves the shift register. As a consequence, all subsequent decryptions (i.e., decryptions of $y_{i+\kappa+}$...) are again correct.

3.

---

4. We want to calculate the number of non-negative integers less than $n=p^a$ that are relatively prime to n. As in many cases, it turns out to be easier to calculate the number that are *not* relatively prime to n, and subtract from the total. List the non-negative integers less than p^a: 0, 1, 2, …, p^a-1; there are papa of them. The numbers that have

a common factor with p^a (namely, the ones that are not relatively prime to n) are the multiples of p: 0, p, 2p, …, that is, every pth number. There are thus $p^a/p=p^{a-1}$ numbers in this list, so $\phi(p^a)=p^a-p^{a-1}$.

5.

We can do it by induction. Note that

$$\binom{p}{k} = \binom{p-1}{k} + \binom{p-1}{k-1}$$

is divisible by p. Therefore,

$$\binom{p-1}{k} \equiv -\binom{p-1}{k-1} \mod p$$

so for induction step, assuming that

$$\binom{p-1}{k-1} \equiv (-1)^{k-1} \mod p$$

you easily deduce

$$\binom{p-1}{k} \equiv (-1)^{k} \mod p.$$

The base case is trivial to check.

---

6. The set {1,2,…,p−1} is a restricted set of residues mod p. If a is any element of this set, then: {a,2a,…,(p−1)a} is also a restricted set of residues mod p. So, exactly one element of the second set is equivalent mod p to 1. So, we have shown that for each $a\in\{1,\ldots,p-1\}$ there is exactly one $b\in\{1,\ldots,p-1\}$ such that:

$$ab\equiv 1 \pmod p$$

Now we check if it can be a=b. This is equivalent to:

$$a^2\equiv 1 \pmod p \Leftrightarrow p\mid a^2-1 \Leftrightarrow p\mid a-1 \text{ or } p\mid a+1 \Leftrightarrow a=1 \text{ or } a=p-1$$

We conclude that for each $a\in\{2,\ldots,p-2\}$ there is exactly one $b\in\{2,\ldots,p-2\}$ so that:

$$ab\equiv 1 \pmod p,\ a\neq b$$

So, the numbers 2,…,p−2 can be seperated into (p−3)/2 pairs, so that the product of the two numbers of each pair is equivalent (mod p) to 1,and therefore:

$$2\cdots(p-2)\equiv 1 \pmod p$$

Therefore:

$$(p-1)!=1\cdot 2\cdots(p-2)\cdot(p-1)\equiv 1\cdot 1\cdot(p-1)\equiv -1 \pmod p$$

---

7. If a prime p has the form 3k+1, k can't be odd, because then 3k+13k+1 would be even, and 2, the only even prime, is not of the form 3k+1. Therefore, $p=3\times(2k')+1=6k'+1$, for some integer k'.

8.

Proof by induction:

$2^3-2=8-2=6$ 6 is indeed divisible by 3

Now for the induction part → show that if n is divisible by 3, then n+1 is too

$(n+1)^3-(n+1) =(n^3+3n^2+3n+1)-(n+1) =n^3+3n^2+2n$

$=n*(n^2+3n+2) =n*(n+1)*(n+2)$

That is a product of 3 consecutive integers. Of 3 consecutive integers, at least one is divisible by 3. Therefore the product is also divisible by 3.

we defined n to be divisible by 3. We showed for 2 this is true. Therefore by induction it is true for 3. Therefore it is true for 4 and so on. Thus that is true for any n>=2