Aria Javani

9725303

1:

a.advantages:

- no block synchronization between sender and receiver is required
- bit errors caused by noisy channels only affect the corresponding block but not succeeding blocks
- Block cipher operating can be parallelized
- advantage for high-speed implementations

disadvantages:

- ECB encrypts highly deterministically
- identical plaintexts result in identical ciphertexts
- an attacker recognizes if the same message has been sent twice
- plaintext blocks are encrypted independently of previous blocks
- an attacker may reorder ciphertext blocks which results in valid plaintext

b. A prime number is a whole number greater than 1 whose only factors are 1 and itself.

c. Returns the count of natural numbers smaller or equal than the input that are relatively prime to the input.

2:

Operation Mode	Description	Type of result	Data Unit Size
ECB	$y_i = e_k(x_i), i \geq 1$	block	n
CBC	$y_1 = e_k(x_1 \oplus IV)$ $y_i = e_k(x_i \oplus y_{i-1}), i \geq 2$	block	n
CFB	$s_1 = e_k(IV)\ and\ y_1 = x_1 \oplus s_1$ $s_i = e_k(s_{i-1})\ and\ y_i = x_i \oplus s_i, i \geq 2$	stream	$r \leq n$
OFB	$y_1 = e_k(IV) \oplus x_1$ $y_i = e_k(y_{i-1}) \oplus x_i, i \geq 2$	stream	$r \leq n$
CTR	$y_1 = e_k(IV \parallel CTR_i) \oplus x_i, i \geq 1$	stream	n

3 :

first input sequence of our decryption block is IV but as the we proceed IV is shifted one by one and get replaced with feedback bits as long as we haven't reached the deleted or inserted bit decryption works fine but when we get to that point our sequence in generating key will be disrupted and it continues until we get rid of that inserted bit (or deleted bit).As soon as the shift register is shifted enough we get back on the right track and continue to decrypt correctly. since our key and thus our shift register in work is length is K it takes K+1 operation to have bit out of shift register.

4 :

5 :

for every k that $\gcd(n,k)=1$, also $\gcd(n-k,n)=1$ so for every $n>2$ all the numbers relatively prime to n can be matched up into pairs $\{k,n-k\}$, so $\varphi(n)$ is even.

6 :

$$\binom{p-1}{k}=\frac{(p-1)!}{k!(p-k-1)!}=\frac{(p-1)(p-2)\dots(p-k-1)!}{k!(p-k-1)!}\ mod\ p$$

mod p will be distributed in all the parenthesis then

$$\left(\frac{-1}{1}\right)\left(\frac{-2}{2}\right)\left(\frac{-3}{3}\right)\dots\left(\frac{-k}{k}\right)\ mod\ p=(-1)^k\ mod\ p$$

7 .1 :

$$3^{201}=3^{11}\times 3^{11}\times 3^{11}\dots\times 3^{11}\times 3^3$$

$$\xrightarrow{a^p\equiv a\ mod\ p} 1\times 1\times\dots\times 1\times 9\equiv 9$$

7.2 :

first we assume a set of all possible strings of length p and a different characters possible for each string so the count of string will be a^p . among all of these strings there are exactly a strings consisting of exactly one character. with the rest of them we make a necklace with each string then we consider all the strings with that have a same necklace with subset length of p in one group the reason we choose p as size is because a subset of length T should be chosen with the condition of T dividing length of whole string and since the length of strings is prim number of p we shall use p (also not 1 because it's trivial) as the sub string length. so p divides a^p-a and $a^p=a$

8 :

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

n+1, n and n-1 are three consecutive numbers one of which is divisible by 3 for sure.

9 :

if a n divides ab then n and ab should have common prime factors but since n is relatively prime to a, they have no common prime factor so there should be at least one common prime factor in n and b so that n can divide ab. By knowing n and b have common prime factors, n|b.