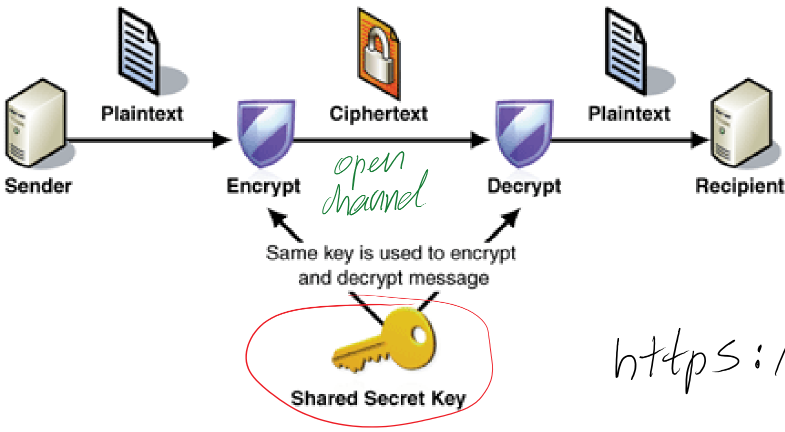
123_003 PublicParameters for KAP



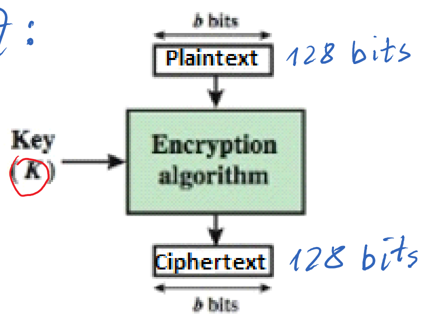
https:// → Diffie-Hellman KAP

A:

M – message to be encrypted

$E(k, M) = C$

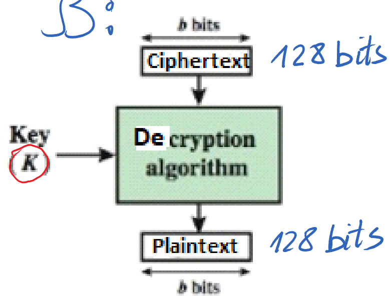
A:



- **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length.

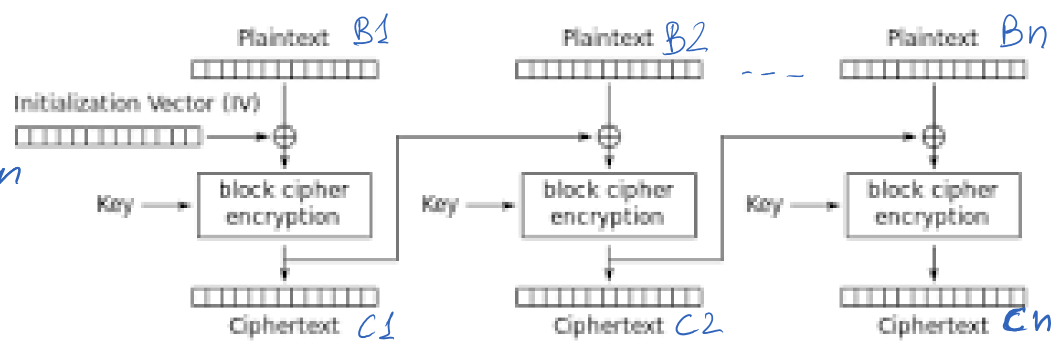
in which messag (plain text) of any finite length is divided into the number of same length block and every block is encrypted with the same relatively short key of length 128 bits, 192 bits, 256 bits or the similar length

B:



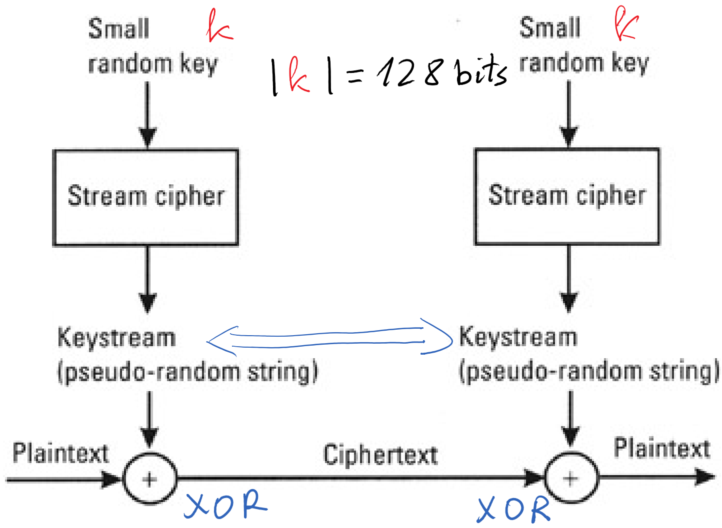
$D(k, C) = M$

IV - is open



Cipher Block Chaining (CBC) mode encryption

$AES-128-CBC \quad : \quad |B1| = |B2| = \ldots = |Bn| = 128$ bits



- A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. Examples of classical stream ciphers are the auto keyed Vigenère cipher and the Vernam cipher.

Diffie-Hellman Key Agreement Protocol - KAP

Public Parameters $= (p, g) = PP$

`>> p = genstrongprime(28)` // $|p| = 28$ bits

To establish KAP Public Parameters - PP are required.

$p = 11$: defines the set of integers $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$

$\mathbb{Z}_p^* = \{1, 2, 3, \ldots, 10\}$ with defined operations mod 11.

Let us fix p - as a prime, then any integer z could be expressed in the form

$$\boxed{z = t \cdot p + r}$$

Let $p = 11$ and $z = 37 \Rightarrow z = 3 \cdot 11 + 4$

$37 \bmod 11 = 4$

$$\boxed{z \bmod p = r}$$

$$\begin{array}{r|l} 37 & 11 \\ \hline 33 & 3 \\ \hline 4 & \end{array} \qquad \begin{array}{r|l} t \cdot p + r & p \\ \hline - t \cdot p & t \\ \hline r & \end{array}$$

$\mathbb{Z}_{11}^* = \{1, 2, 3, \ldots, 10\}$ * mod 11 : it is a group of integers mod p.

$2 \cdot 6 \bmod 11 = 12 \bmod 11 = 1$

Multiplication Tab.		Z11*								
*	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9

3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

$$\begin{array}{r|l} -32 & 11 \\ \underline{22} & 2 \\ 10 & \end{array}$$

$2^5 \bmod 11 = 2\cdot 2\cdot 2\cdot 2\cdot 2 \bmod 11$
$= 32 \bmod 11 = 10$

Power Tab.		Z11*									
^	0	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	5	10	9	7	3	6	1
3	1	3	9	5	4	1	3	9	5	4	1
4	1	4	5	9	3	1	4	5	9	3	1
5	1	5	3	4	9	1	5	3	4	9	1
6	1	6	3	7	9	10	5	8	4	2	1
7	1	7	5	2	3	10	4	6	9	8	1
8	1	8	9	6	4	10	3	2	5	7	1
9	1	9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1	10	1

gen. 1

gen. 2

gen. 3

gen. 4

$\Gamma = \{2, 6, 7, 8\}$

$|\mathbb{Z}_{11}^*| = 10$

$|\Gamma| = 4$

The probability (chance) to find a generator in $\mathbb{Z}_{11}^*$ (or in $\mathbb{Z}_p^*$) is approximately the following

$$\text{Prob}(g \text{ is a generator in } \mathbb{Z}_p^*) \approx 4/10 = 2/5$$

$g \leftarrow \text{randi}; \quad g \in \{2, 3, 4 \ldots\}$

$$PP = (p, g)$$

For the security reason $p \approx 2^{2048}$; $|p| \sim 2048$ bits.

$1\,K \to 2^{10} = 1024 > 10^3 = 1000$

$1\,M \to 2^{20}$ ----- $> 10^6$

$1\,G \to 2^{30}$ ----- $> 10^9$

$1\,T \to 2^{40}$ ----- $> 10^{12}$

$2^{2048} \sim 10^{700}$

$\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}; \quad \bullet \bmod p$

```
>> 2^28-1
ans =  268435455
```

p = 264043379 Check that *p* is strong prime;	**p = 268435019**

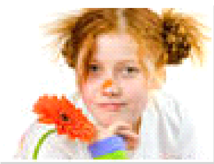
$g = 2$	$g =$

C.5.3 Finding generators.
We have to look inside Z_P* and find a generator. How?
Even if we have a candidate, how do we test it?
The condition is that g is a generator would take $|Z_P^*|$ steps to check: $p \sim 2^{2048}$ --> $|Z_P^*| \sim 2^{2048}-1$.
In fact, finding a generator given p is in general a hard problem.

We can exploit the particular prime numbers names as **strong primes**.
If p is prime and $p=2q+1$ with q prime then p is a **strong prime**. Ex. $p = 11 = 2 \cdot 5 + 1$
Note that the order of the group Z_P* is $p-1=2q$, i.e. $|Z_P^*|=2q$. $q = (p-1)/2$
Fact C.23. Say $p=2q+1$ is prime where q is prime, then g in Z_P* is a generator of Z_P*
iff $g^q \neq 1 \bmod p$ and $g^2 \neq 1 \bmod p$.

Testing whether g is a generator is easy given strong prime p.
Now, given $p=2q+1$, the generator can be found by randomly generation numbers $g<p$ and verifying Fact C.23. The probability to find a generator is ~0.4.

How to fing more generators when **g** one is found?
Fact C.24. If g is a generator and i is not divisible by q and **2** then g^i is a generator as well, i.e.
If g is a generator and $\gcd(i,q)=1$ and $\gcd(i,2)=1$, then g^i is a generator as well.



secret random number
>> u = randi ($p-1$)
$A = g^u \bmod p$
>> A = mod_exp(g, u, p)

$\xrightarrow{A}$

secret random number
>> v = randi ($p-1$)
$B = g^v \bmod p$
>> B = mod_exp(g, v, p)

$\xleftarrow{B}$

$k_{AB} = B^u \bmod p$ ==== k ==== $k_{BA} = A^v \bmod p$

$k_{AB} = B^u \bmod p = (g^v)^u \bmod p = g^{vu} \bmod p =$
$= g^{uv} \bmod p = (g^u)^v \bmod p = A^v \bmod p = k_{BA}$

$$k_{AB} = k_{BA} = k$$

till this place