protocolo confidencialidad usando criptografia simetrica.

a:k------>b:k

m C

1.-los entes a y b deben acordar una llave

2.-a: Ck(m)=c

3.-a----->b:m

4.-b:Dk(C)=m

protocolo confidencialidad usando criptografia simetrica.

A -----> B

m C m

0.-receptor:kpriv,kpublic,descifrar

1.-A:Ckpublic(m)=c

2.-A-->B:C

3.-B:Dkpriv(c)=m

protocolo de integridad

1.A:H(m)=Hm

2.A--->B:{m;Hm} [H] referido a hash

3.b:H(m)=hB

4.B: si Hm=HB=>m es valido

sino =>m se rechaza

protocolo de autenticacion

mismos que los de confidencialidad

protocolo de no repudio

M M

A G B

1.A-🡪G:M

2.G-🡪B:M

Firma Digital

Es un protocolo de autenticación y no repudio

A --------------🡪 B

Doc

1.

2.

3.

Firma digital con integridad

1.-

2.A:H(Cdoc)=Hm

3.A-----🡪B:{,}

4.B:H()=

SI HB =

SINO SE RECHAZA

Certificado digital

EMISOR RCEPTOR

A B

FIRMA DIGITAL CERTIFICADO DIGITAL

AUTENTICA Y NO AUTENTICA Y NO

REPUDIO REPUDIO

El certificado digital es un archivo emitido por un tercero en confianza que contiene la llave publica del ente a certificar. Este tercero llamado autoridad certificadora, certifica la autenticación de la llave y del ente propietario de la llave.

SIM: Mas rapida

ASIM: Robusta

Protocolo de intercambio de llave

1.A:;B:------ >, ,

2.A:

3.A------- >B:C

4.B: