<u>ASSIGNMENT -17</u>

Q1. Explain the data encryption standard (DES) and Rivest –Shamir-Adleman (RSA) Algorithms .

ANS:

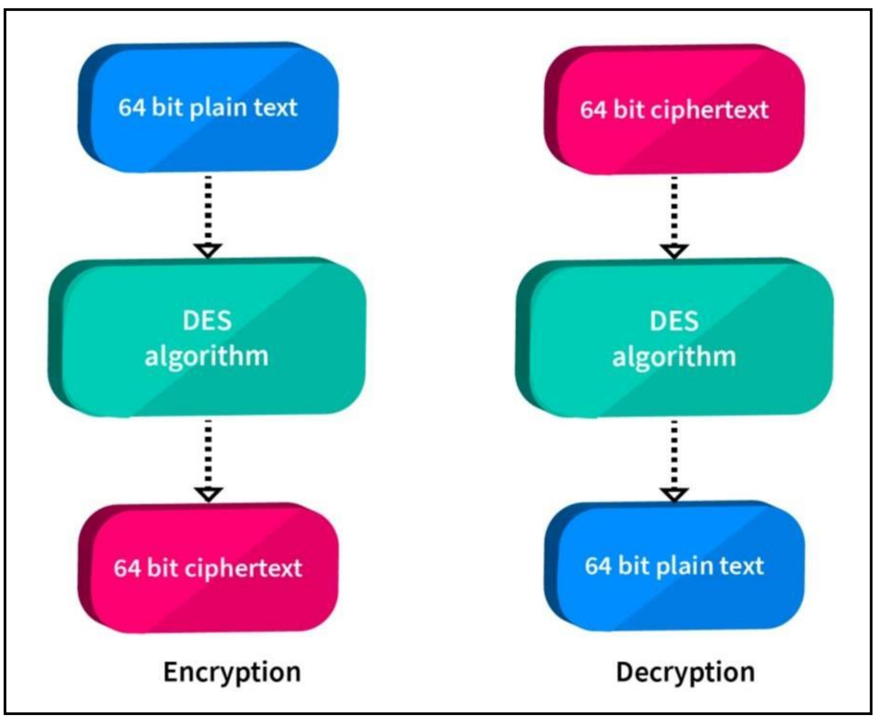
Algorithm

DES operates using a 56-bit key and follows a specific sequence of processing steps known as the Feistel structure

• Key Generation Generates 16 subkeys, each 48 bits in length, from the initial 56-bit key.

• Initial Permutation (IP) The 64-bit input block of plaintext undergoes an initial permutation that rearranges the bits to produce a permuted input.

• Rounds The permuted block is then subject to 16 rounds of processing which involve expansion, substitution, and permutation.



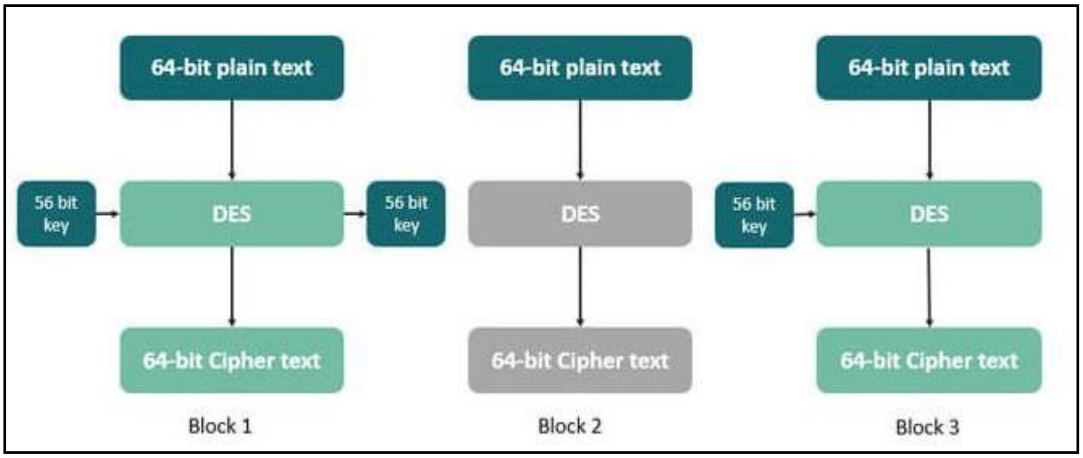
Algorithm

• Expansion Each 32-bit half-block is expanded to 48 bits using an expansion permutation, mixed with a round key.

• Substitution After mixing, the block passes through a series of S-boxes (substitution boxes) that transform the expanded half-block into a 32-bit output.

• Permutation Finally, a permutation function that rearranges the bits to produce the pre-output.

• Final Permutation The final output is then produced by reversing the initial permutation to produce the final 64- bit block of ciphertext.



DataEncryptionStandard

PlainText"1101011010111011"

Step1ConvertPlainTexttoBinary
Binary"1101011010111011"

Step2InitialPermutation(IP)

Original1101011010111011

Permuted1011101111010110(justswappinghalvesforsimplicity)

Step3RoundProcessing(ExampleofRound1)
Expansion

RightHalf11010110

Expanded Right Half (Duplicating Every SecondBit)
11110011 01100110

- 1 (firstbit of righthalf) →duplicate→11
- 1(secondbit, alreadyduplicated)→duplicateagain→11
- 0(thirdbit)→duplicate→00
- 1 (fourthbit)→duplicate→11

- 0 (fifthbit)→duplicate→00
- 1 (sixth bit)→duplicate→11
- 1(seventhbit) →duplicate→11
- 0(eighthbit,last)→duplicate→00

DataEncryptionStandard

KeyforRound1

RoundKey0011001111001100

KeyMixing(XOR)
ExpandedRightHalf1111001101100110

RoundKey0011001111001100

XOROperation

- 1⊕ 0 = 1
- 1⊕ 0 = 1
- 1⊕1= 0
- 1⊕ 1 = 0
- 0⊕ 0 = 0
- 0⊕ 1 = 1
- 1⊕ 1 = 0
- 1⊕0= 1
- 0⊕1= 1
- 1⊕1= 0
- 1⊕0= 1
- 0⊕0= 0
- 0⊕1= 1
- 1⊕1= 0
- 1⊕0= 1
- 0⊕0= 0

SubstitutionwithS-Boxes(usingsimplifiedS-boxes)
Input110000001010 1010

S-BoxesOutput(hypothetical)10101111
(Each4bitsofinputarereducedto2bitsofoutputforsimplicity)

Permutation(simplifiedpermutation)Input10101111
Permuted11111010

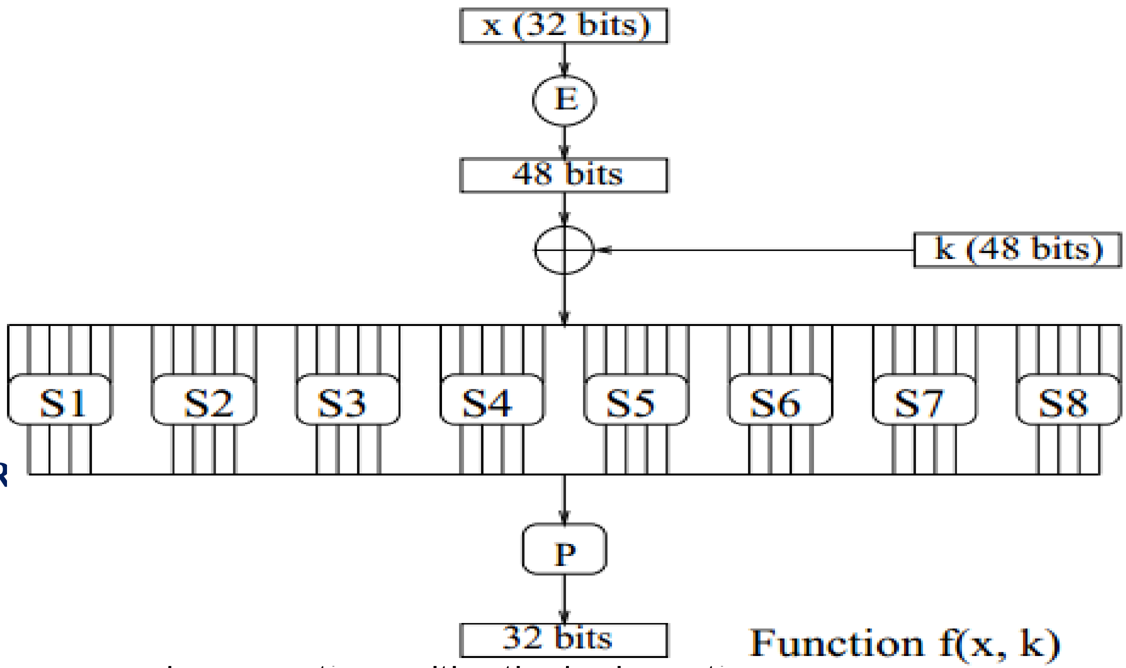
Swapping
LeftHalfOriginal10111011

NewRightHalfAfterProcessing11111010
NewState1111101010111011

Step 4 final permutation

Input 11111010 10111011

Final permutation 10111011 11111010(reverse of initial ,just swapping halves)

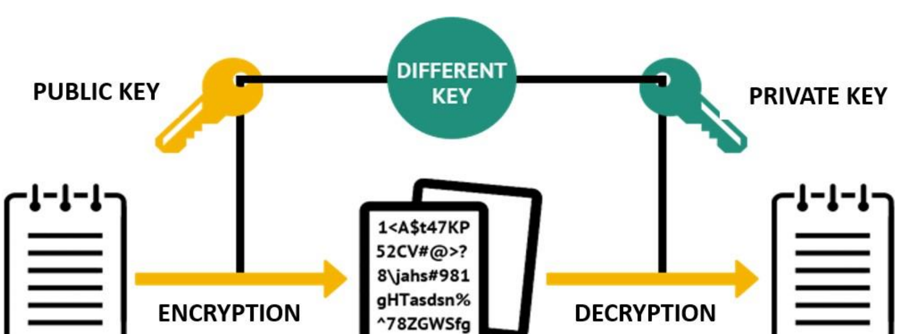


R

one for encryption andtheotherfordecryption.

- The key used for encryption is the public key,and the key used for decryption is the privatekey.

But,ofcourse,boththekeysmustbelongto thereceiver



For example, if Alice needs to send a message toBob, both the keys, private and public, must belongtoBob.

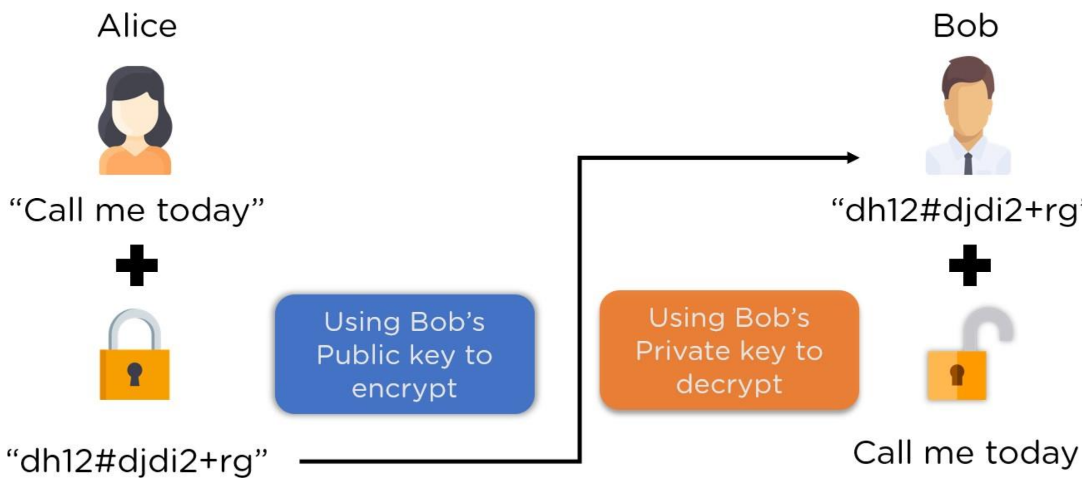
Theprocessfortheimageisasfollows

- Step1AliceusesBob'spublickeytoencryptthemessage.

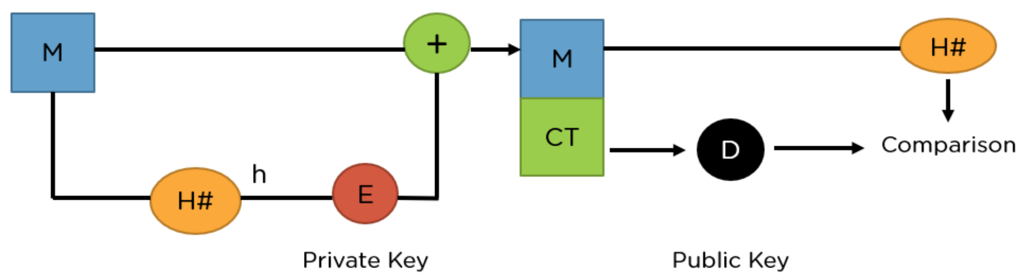
- Step2 Theencryptedmessage issenttoBob.

- Step3Bobuseshisprivatekeytodecryptthe message.

This eliminates the need to exchange any secret keybetween sender and receiver, thereby reducing thewindowofexploitation.



RSA algorithm is a public-key signature algorithmdeveloped by Ron Rivest, Adi Shamir, and LeonardAdleman.



Two broad components Involved in RSA are

- Key Generation Generating the keys to be used for encrypting and decrypting the data to bee changed.

- Encryption/Decryption Function The steps thatneed to be run when scrambling and recoveringthedata.

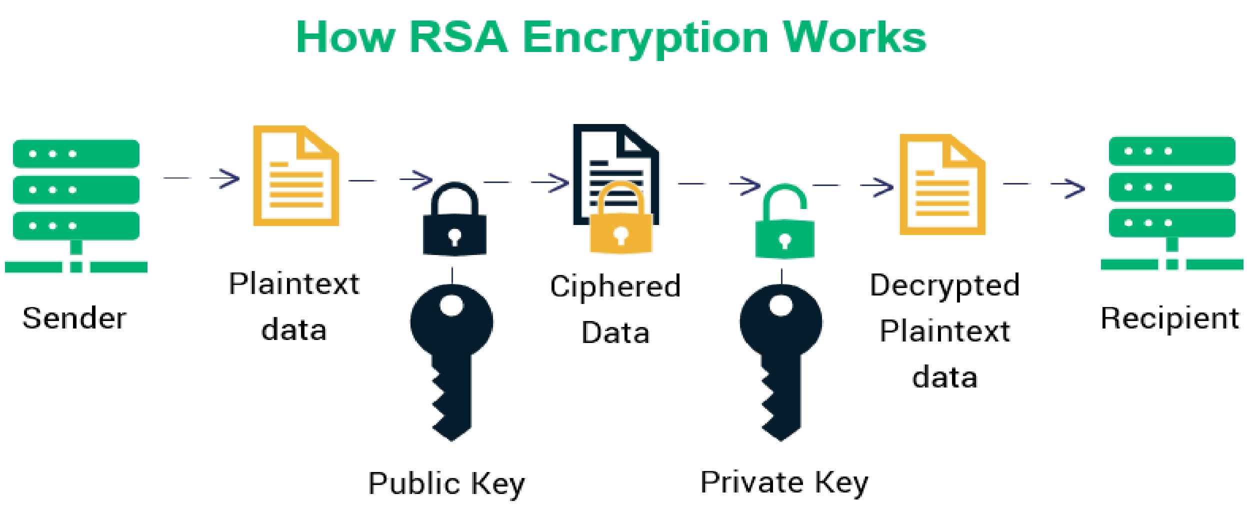
- **StepsinRSAAlgorithm**
- KeyGeneration
  - Generate public and private keys before runningthefunctionstogenerateyourciphertextandplaintext.Theyusecertainvariablesandparameters,allofwhichareexplainedbelow
    - Choosetwolargeprimenumbers(pandq)
    - Calculaten=p*qandz=(p-1)(q-1)
    - Chooseanumberewhere1<e<z
    - Calculated=e-1mod(p-1)(q-1)
    - Bundleprivatekeypairas(n,d)
    - Bundlepublickeypairas(n,e)
- **StepsinRSAAlgorithm**
- **Encryption/DecryptionFunction**
- Once the keys are Generated, pass the parameters tothefunctionsthatcalculatetheciphertextandplaintextusingtherespective key.
  - Iftheplaintextism, ciphertext= memodn.
  - Iftheciphertextisc,plaintext=cdmodn

- **Example**
- Considerp = 17 andq=13.

- Valueofecanbe5asitsatisfiesthecondition1<e<(p-1)(q-1).
- N=p *q=221
- D= e-1mod(p-1)(q-1)=29
- PublicKey pair=(221,5)
- PrivateKeypair=(221,29)
- Iftheplaintext(m)valueis10,youcanencryptitusingthe formulamemodn=82.
- Todecryptthisciphertext(c)backtooriginaldata,
  youmust usetheformulacdmodn=29

AdvantagesofRSA

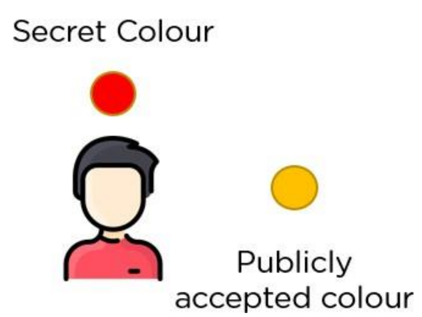
- NoKeySharing
- ProofofAuthenticity
- FasterEncryption
- DataCan'tBeModified



Q2. EXPLAIN DIFFIE –HELLMAN KEY EXCHANGE ALGORITHM WITH AN EXAMPLE .

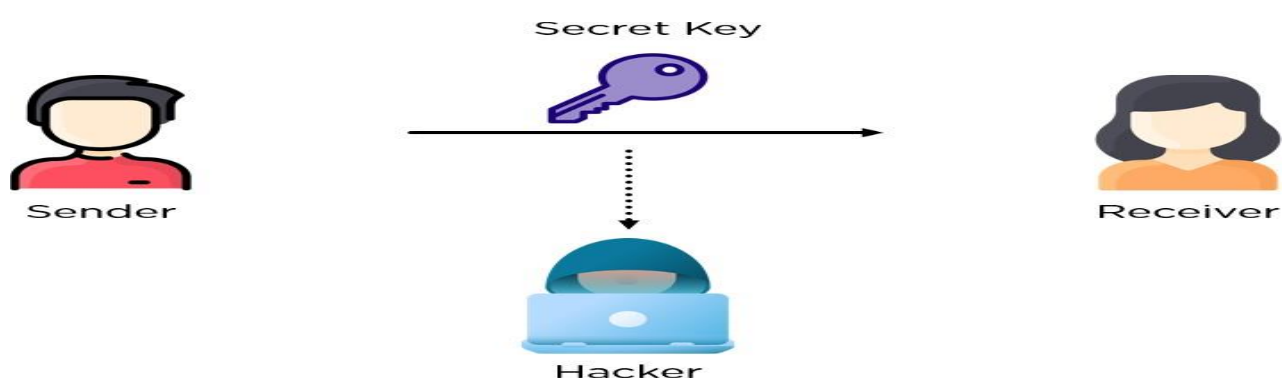
Ans.

The Diffie Hellman algorithm solves this problemusingone-wayfunctionsthatenableonlythesender and receiver to decrypt the message usingasecretkey.



Step1 Letthetwouserschooseapubliclyacceptedcolortheybothagreeto.

Theymustalsodecideonaprivatecolorwhichistobekeptasasecret.

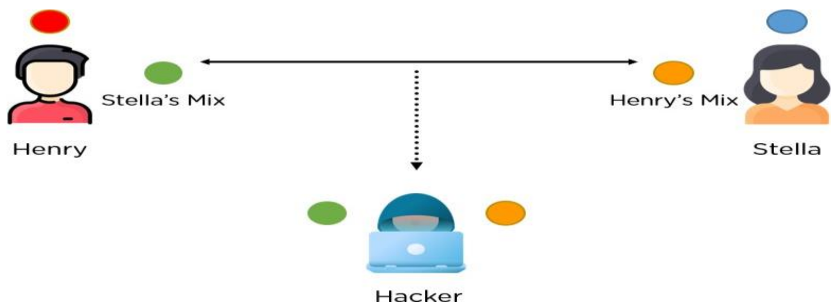


Step2

Theprivateandpubliccolorsaremixedoneachsidetoform anewlyacquiredcolormixture.

Step3

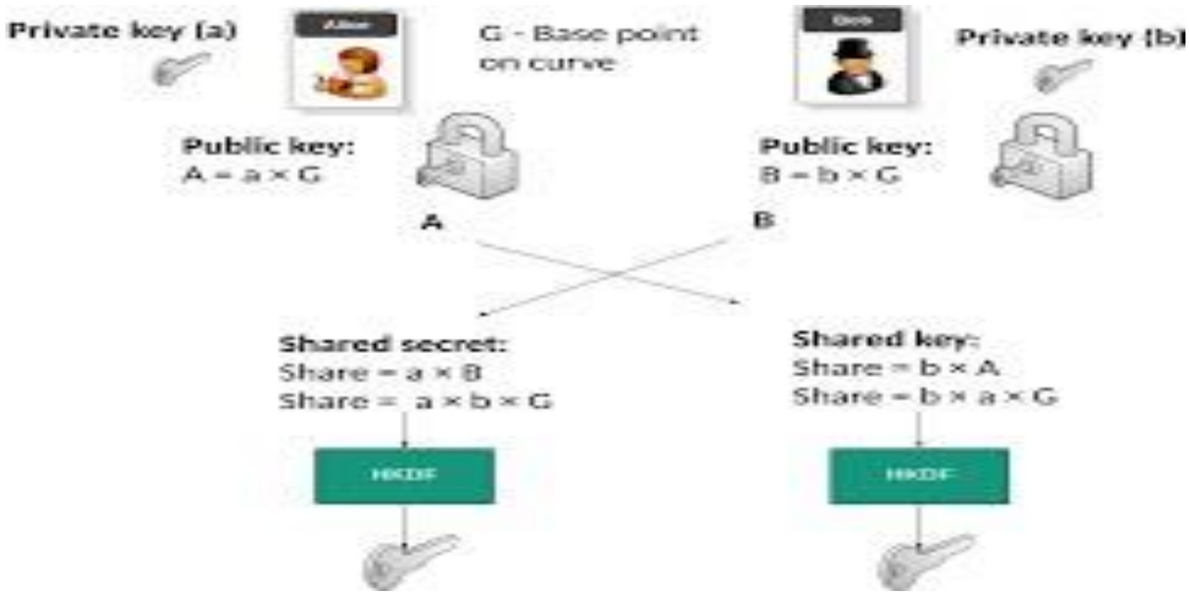
Theythenexchangethemixtureamongtheusers over an insecure communication channel, eventhoughitmaybeopenforhackerstointercept.



Step 4

The private colors are then mixed with thereceived mixture to finally acquire the actual secretcolor(key).

- Elliptic Curve Diffie-Hellman(ECDH)isa cryptographic protocol based on Elliptic CurveCryptography(ECC).
- It provides a method for two parties to establishasharedsecretkeyoveraninsecurecommunicationchannel.
- ECD His an extension of the traditional Diffie-Hellman key exchange protocol, offering severaladvantagesintermsofsecurityandefficiency.
- **Advantages**
    - SmallerKeySizes
    - FasterKeyGeneration
    - StrongerSecurity



Q3.EXPALIN DIGITAL SIGNATURE ALGORITHM WITH A EXAMPLE .

Adigital signature is an e-signature that is backedbyadigitalcertificate.

A digital signature is an electronic, encrypted,stamp of authentication on digital informationsuch as email messages, macros, or electronicdocuments.

Asignatureconfirmsthattheinformationoriginated from the signer and has not beenaltered.

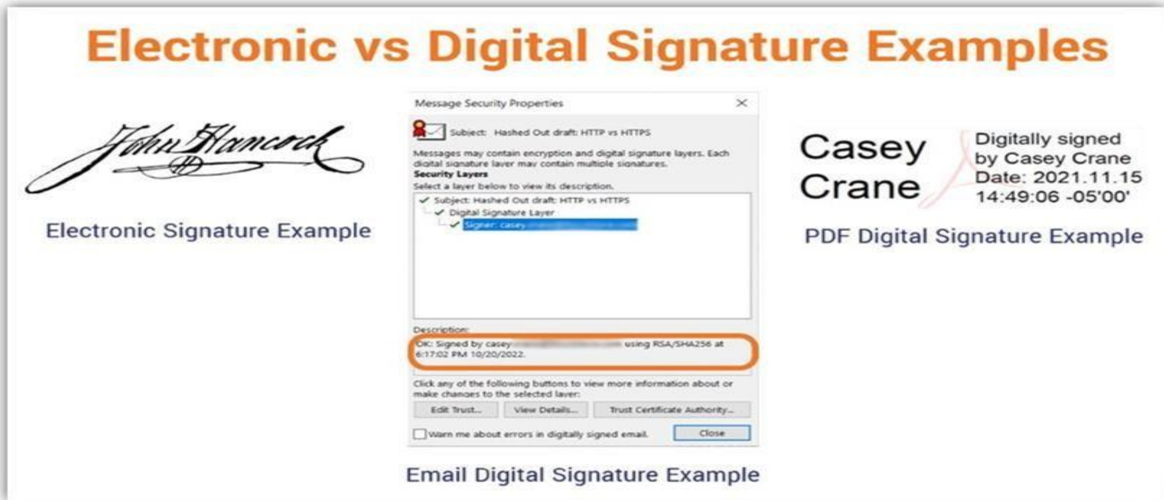
DigitalSignatureinCryptographyisavaluecalculated from the data along with a secretkeythatonlythesigneris awareof.

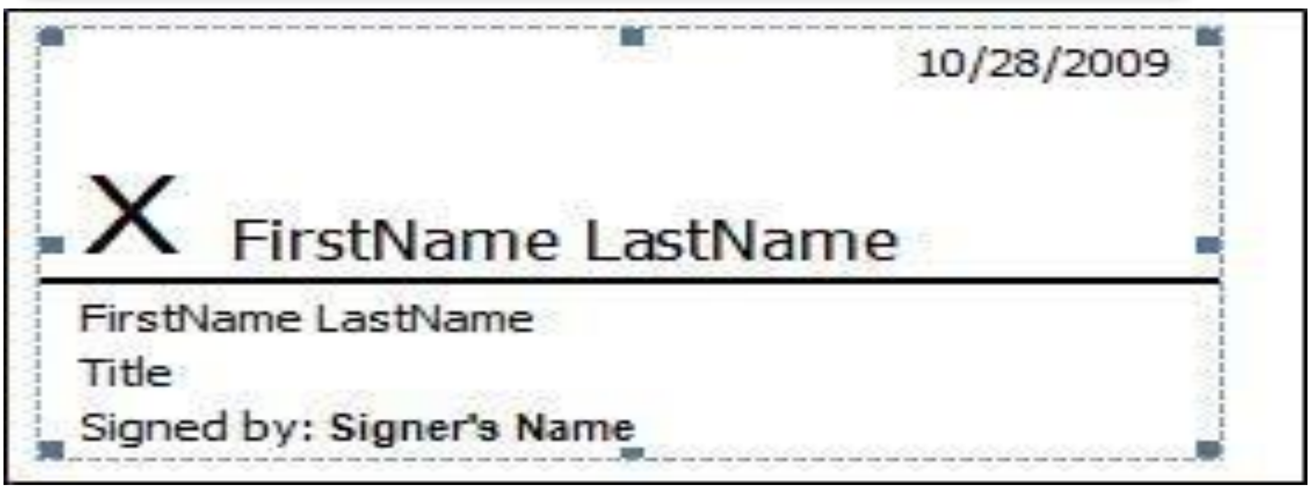
BenefitsofDigitalSignatures

- TrustedandCompliant
- Protected
- UniquetotheUser
- EasytoValidate

  - Digitalsignaturealgorithmsarecryptographicprotocolsthatprovide ameansforvalidatingtheauthenticityandintegrityofdigitalmessages ordocuments.

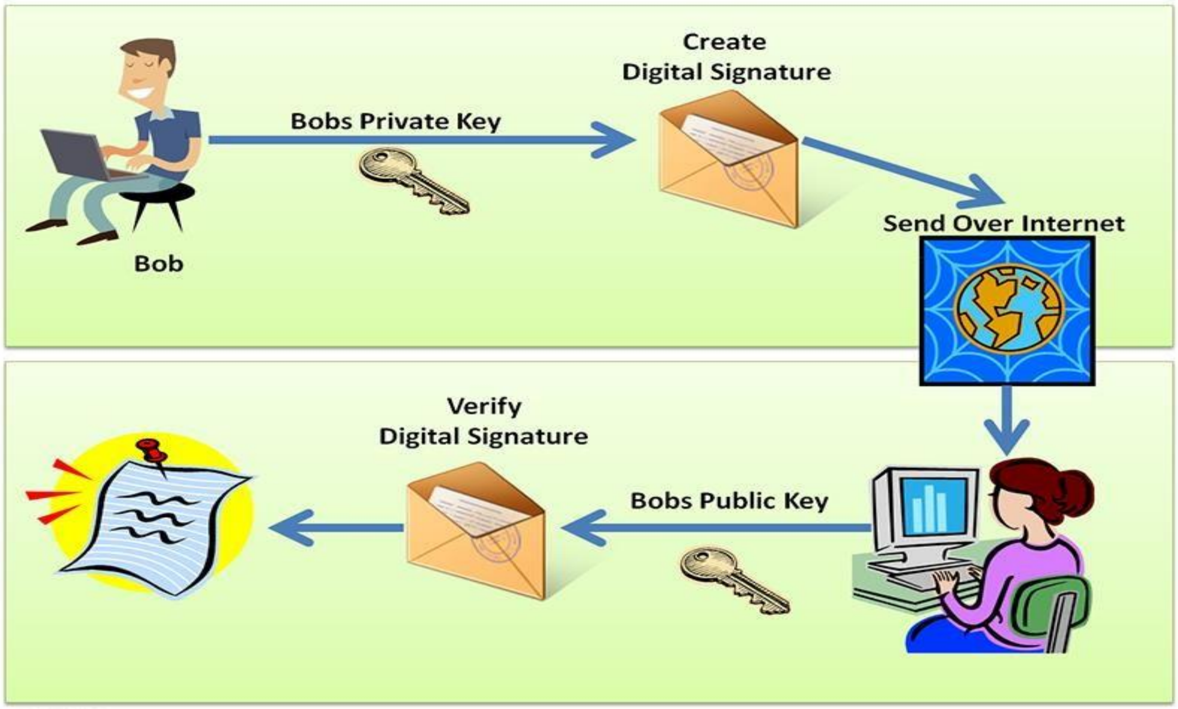
- Digitalsignaturesarewidelyusedinsoftwaredistribution, financial transactions, and other areaswhere it is crucial to ensure that communicationsaresecure andcannotbe tamperedwith





Digital Signature Process:

- Step1:GeneratePrivateKeyandPublicKey
- Step2:CreateDigitalSignature
- Step3:CommunicateThroughChannel
-
- Step4:DecryptUsingPrivateKey
- Step5:VerifytheDigitalSignature



DigitalSignatureAlgorithm(DSA)

DevelopedbytheU.S.NationalSecurityAgency(NSA)andstandardizedbytheNationalInstituteofStandardsandTechnology(NIST),DSAisaFederalInformationProcessingStandardfor digitalsignatures.

Itwasdesigned toprovide an alternativetoRSAandusesadifferentmathematicalapproachbasedondiscretelogarithms

Process

- **Signing** DSA uses a private key along with aset of predefined parameters to produce twoquantities, labeled as r and s, derived from thehashofthemessage.

- **Verification**Theverifierusesthesigner'spublickeyandthesamepredefinedparametersstocomputetwovaluesthatshouldmatch the original r and s if the signature isvalid.

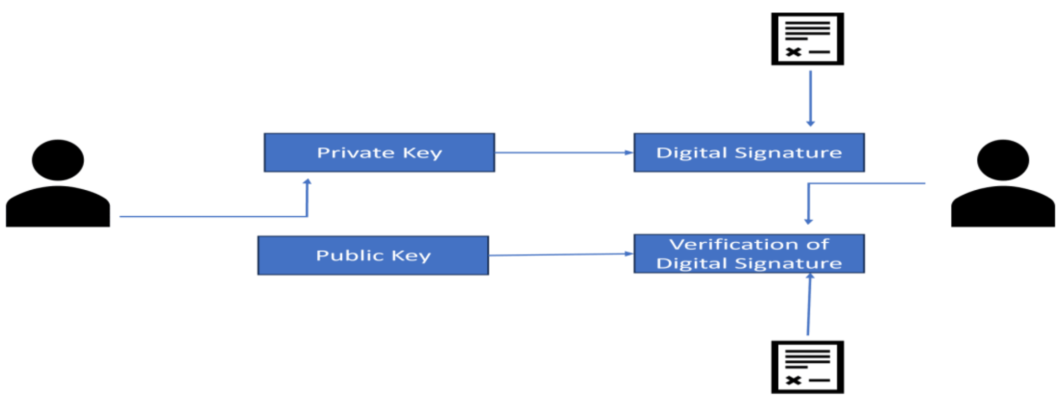
- Generate a prime number q, a primenumber(where$p-1$isamultipleof$q$),andanumber$g$(where$g$isa$p$-throotof1 mod$p$).

- Choose a private key x randomly from N [1,−1].

- Calculatethepublickey$y=g^x$mod$p$.

Signing:

- Generatearandomper-messagevalue$k$from[1,q−1].
- Compute$r$= (gk mod p) mod q.
- Compute$s=k^{-1}$((m)+ xr) $modqwhereH$(m)is the hash of the message.
- Compute$w=s^{-1}modq$.
- Compute u_1=(m). w mod q and u2 = $r.wmodq$
- Compute$v$= (($g^{u1}.y^{u2}modp$)
- SignatureisValidif$v=r$.



Advantages

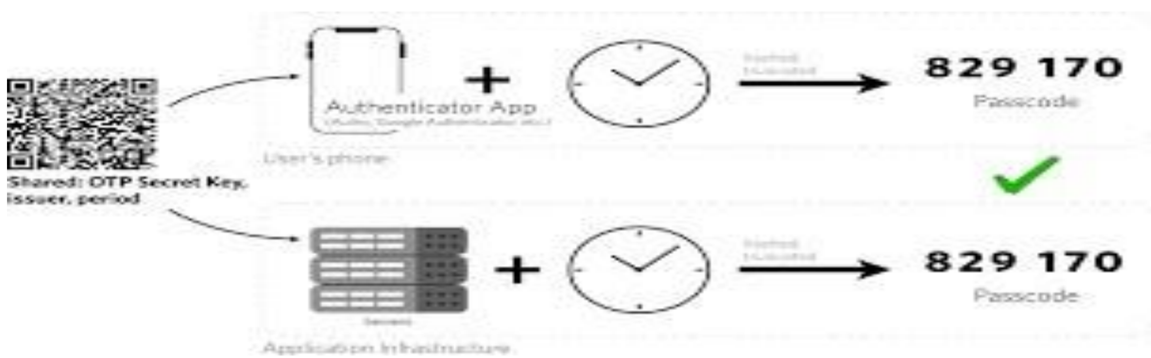
- Efficiency
- KeySizeandSignatureLength
- SecurityFocus

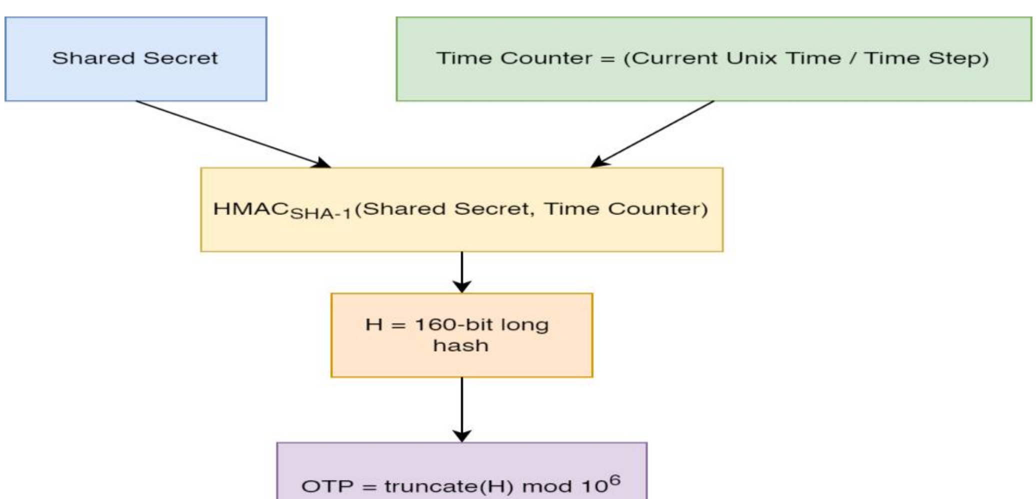
Disadvantages

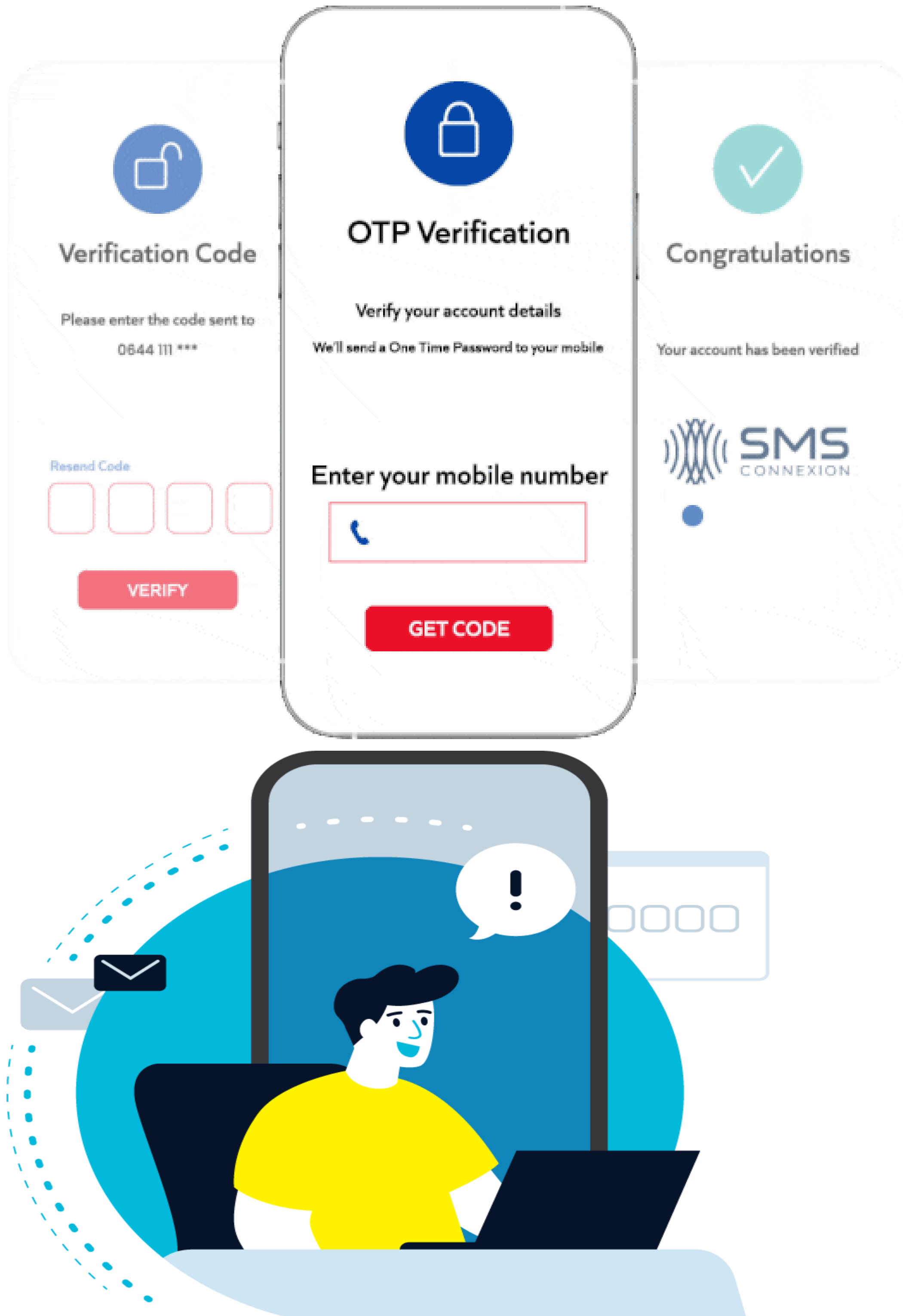
- Non-versatility
- SensitivitytoRandomNumberQuality
- Pre-computationAttacks

Q4. Time based OTP (TOTP)

- **Time-basedOTP(TOTP):**GeneratesOTPsby combining a secret key with the currenttimestampandapplyingacryptographichashfunction.







Verification Code
Please enter the code sent to
0644 111 ***
Resend Code
VERIFY
OTP Verification
Verify your account details
We'll send a One Time Password to your mobile
Enter your mobile number
GET CODE
Congratulations
Your account has been verified
SMS
CONNEXION

- Time-BasedOne-TimePassword(TOTP)algorithmsareacornerstoneofmoderncybersecurity,offeringadynamicandsecuremethodofauthenticating useridentities.

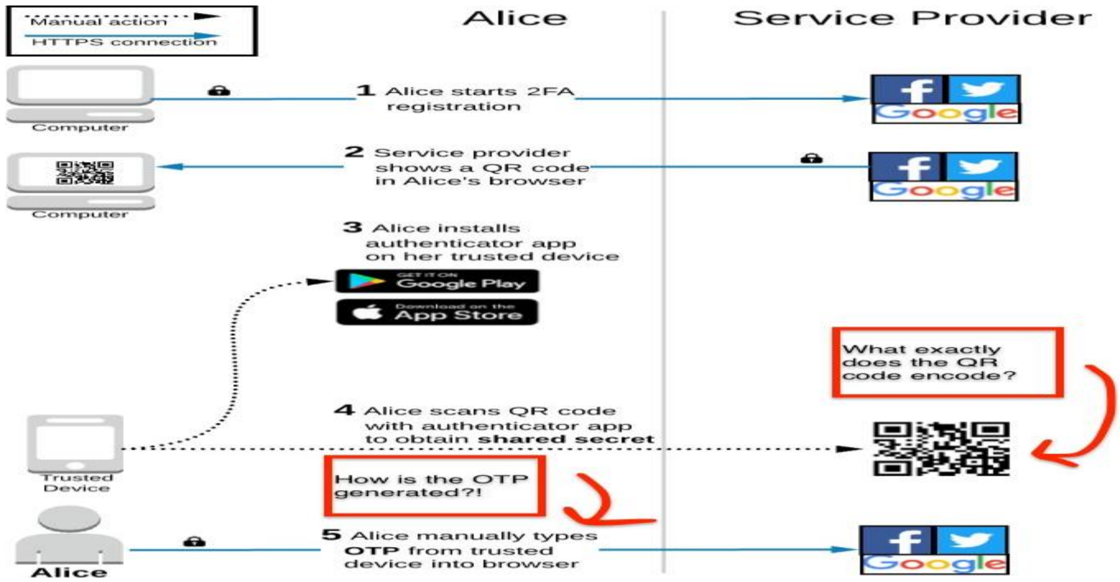
- The foundation of TOTP is built upon theHMAC-Based One-Time Password (HOTP)algorithm, but where HOTP passwords arevaliduntilused,TOTPpasswordsexpireafterasetduration.

Due to its robustness and simplicity, TOTPhasbecomeubiquitousinmulti-factorauthentication(MFA)systems,especiallyinapplicationsrequiringhighsecuritywithrelativelyeasyimplementation .

- EnhancedSecurity
- MitigationofReplayAttacks
- UserConvenience
- Cost-Effective
- RegulatoryCompliance

WideAdoptionandStandardization

- OnlineBanking
- CloudServices
- VPNAccess
- E-commercePlatforms



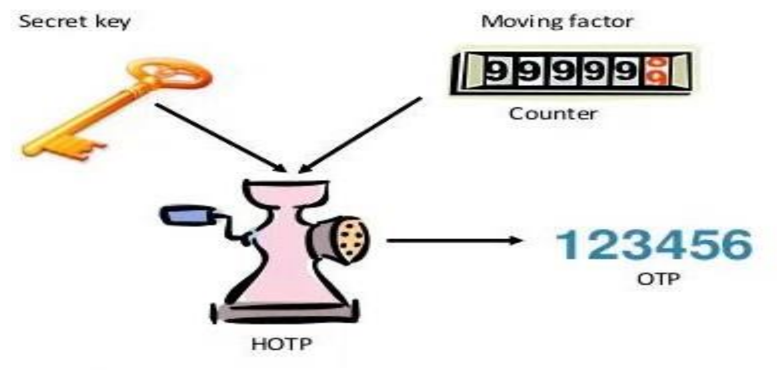
HMAC-BasedOne-TimePasswordAlgorithm(HOTP)

- HMAC-Based One-Time Password (HOTP)is a cornerstone technology in the realm ofcryptographicauthentication.

- TheoperationofHOTPinvolvesanincrementing counter that both the clientand the server maintain, which serves asthemovingfactorinthepasswordgenerationprocess.

- HOTP'sstrength lies in its flexibilityandsecurity.

- AdoptionofHOTPhasbeenwidespreadacrossvarioussectorsduetoi tsrobustness and the ease with which it canbeintegratedintoexistingsecurity



ApplicationsofHMAC-BasedOne-TimePasswordAlgorithm(HOTP)

- BankingandFinancialServices
- CorporateAccessControl
- OnlineGamingandServices
- HealthcareSystems