Université: BadjiMokhtarAnnaba **Semestre:**02
Niveau:L3 **Année:**2024/2025

Module:SécuritéInformatique

SérieTD1

Question1: Imaginezunmondesanssécuritéinformatique.Quelsseraientlesimpactssurlaviequotidienne des individus, des entreprises et des États ?

Àpartirdecetteréflexion,quelssontlesprincipauxmotivationsquijustifientlanécessitédelasécurité informatique ?

Question2:Déterminezsichaqueincidentrelèvedelasécuritéinterneouexterne,puisproposezunesolution efficace pour éviter qu'il ne se reproduise à l'avenir.

1. Unemployétéléchargeparerreurunlogicielinfectédepuissonordinateurprofessionnel
2. Unhackertented'arrêterlaplateformed'uneentrepriseviauneattaquededénideservicedistribué (DDoS).
3. Unmotdepassefaibled'uncadresupérieurestpiratéetutilisépouraccéderauxdonnées confidentielles.
4. Une-mailfrauduleux(phishing)cibleplusieursemployéspourvolerleursidentifiants.
5. Untechnicieneninterne copie desfichierssensiblessansautorisation.
6. Unemployé perdsonordinateurportableprofessionnelcontenantdesdonnéessensibles

Question3: Analysesdesrisqueset préjudices

1. Expliquez avec vos propres mots les concepts suivants en sécurité informatique : **vulnérabilité, menace, attaque, préjudice, probabilité et risque**.
2. Illustrer votre explication avec un exemple concret lié à une **injection SQL**, en tenant compte du fait que vous devez concevoir un site web ou une application.
3. **Calcul :**Si la probabilité d'une attaque est de 30 % et que le préjudice potentiel est estimé à 100 000 €, quel est le risque associé ? Utilisez la formule d'estimation du risque.

Question4 : Politiquesdesécurité

1. Qu'est-cequ'unepolitiquedesécuritéetquelssontsesobjectifs?
2. Associezchaquescénarioci-dessousàl'objectifde sécuritéqu'ilcompromet:
   a. Unserveurtombeenpanne,rendantlesdonnéesinaccessiblespendantplusieursheures ( )
   b. Un acteur malveillant accède à une base de données client en exploitant une faille de sécurité(.....)
   c. Unvirusaltère desfichierscritiquessurunserveur.
   d. Unthreatactorutiliselesidentifiantsvolésd'unemployépouraccéderauréseaudel'entreprise ( )
   e. Une transaction financière est effectuée, mais aucun enregistrement de l'utilisateur ne peut en attester (….....)
   f. Unclientnieavoirpasséunecommandeenligne,alorsquelesystèmeprouvelecontraire ( )
   g. Unfichierconfidentielest modifiéentransit parunattaquant (….....)
   h. Unepannedeserveurentraîneunepertededonnées,etilestimpossibled'enidentifierlacause exacte (… .....)

3. Quelle est la différence entre un pare-feu (Firewall), un système de détection d'intrusion (IDS) et un système de prévention d'intrusion (IPS) dans la mise en œuvre d'une politique de sécurité ?

Question5: Attaquesetcontre-mesures

1. Quelleestladifférenceentreuneattaquepassiveetuneattaqueactive?Donnezunexemplepour chaque type.
2. Complétez le tableau suivant en associant chaque type d'attaque à sa catégorie, sa description et un exemple :

Type d'attaque	Catégorie	Description	Exemple
Interception			
Interruption			
Modification			
Fabrication			

Question6: La normeISO 27000

1. Quelestl'objectifprincipaldelanormeISO27000?
2. Quellessontlesprincipalesnormesdelafamille ISO27000etquelestlerôledechaque norme?
3. Quellessontlesquatrephasesdela normeISO27000etquelestl'objectifdechaquephase.

Université: BadjiMokhtarAnnaba **Semestre:**02
Niveau:L3 **Année:**2024/2025

Module:SécuritéInformatique

SérieTD1

Question1: Imaginezunmondesanssécuritéinformatique.Quelsseraientlesimpactssurlaviequotidienne des individus, des entreprises et des États ?

Àpartirdecetteréflexion,quelssontlesprincipauxmotivationsquijustifientlanécessitédelasécurité informatique ?

(Danslecours,premièrepage)

Question2:Déterminezsichaqueincidentrelèvedelasécuritéinterneouexterne,puisproposezunesolution efficace pour éviter qu'il ne se reproduise à l'avenir.

1. Unemployétéléchargeparerreurunlogicielinfectédepuissonordinateurprofessionnel
2. Unhackertented'arrêterlaplateformed'uneentrepriseviauneattaquededénideservicedistribué (DDoS).
3. Unmotdepassefaibled'uncadresupérieurestpiratéetutilisépouraccéderauxdonnées confidentielles.
4. Une-mailfrauduleux(phishing)cibleplusieursemployéspourvolerleursidentifiants.
5. Untechnicieneninterne copie desfichierssensiblessansautorisation.
6. Unemployé perdsonordinateurportableprofessionnelcontenantdesdonnéessensibles

	Scénario	Notionsà discuter	Typede sécurité	Solution
1	Unemployétéléchargeparerreurunlogiciel infectédepuis sonordinateur professionnel.	/	Interne	Formationdesemployéssurla cybersécurité+Miseenplaced'un système derestrictiondes téléchargements.
2	Un hacker tente de pénétrer votre réseau viauneattaquepardénideservice(DDoS).	DoS,How itworks+ DDoS	Externe	Utilisationd'uneprotectionanti-DDoS et d'unpare-feuavancé.
3	Unmotdepassefaibled'uncadresupérieur est piraté et utilisé pour accéder aux donnéesconfidentielles.	Brute force	Interne	Impositiondemotsdepasseforts+ Activationdel'authentificationàdeux facteurs(2FA).
4	Une-mailfrauduleux(phishing)cible plusieurs employés pour voler leurs identifiants.	Phishing	Externe	Filtragedese-mails+Sensibilisationdes employés au phishing.
5	Untechnicieneninternecopiedesfichiers sensibles sans autorisation.	Gestion d'accès	Interne	Surveillancedesaccèsauxfichiers+Mise en place d'une gestion stricte des autorisations.
6	Unemployéperdsonordinateurportable professionnel Contenantdesdonnéessensibles	\	Interne	Lesdonnéessensiblesdoiventêtrestockées dans un endroit (serveur) sécurisé (sécurité physique)

Question3: Analyses des risques et préjudices

1. Expliquez avec vos propres mots les concepts suivants en sécurité informatique : **vulnérabilité, menace, attaque, préjudice, probabilité et risque**.

Une **vulnérabilité** est une faiblesse ou une faille dans un système, un logiciel, un réseau ou un processus qui pourrait être exploitée par une menace.

Une **menace** est tout élément ou événement susceptible d'exploiter une vulnérabilité et de causer un dommage. Une menace peut être intentionnelle (pirate informatique) ou accidentelle (erreur humaine, catastrophe naturelle).

Une **attaque** est l'action concrète menée par une menace pour exploiter une vulnérabilité. Elle peut être technique (virus, phishing, injection SQL) ou sociale (ingénierie sociale).

Le **préjudice** est l'impact négatif causé par une attaque réussie. Cela peut être une perte financière, une atteinte à la réputation, une violation de données, etc.

La **probabilité** est la mesure du risque qu'une menace exploite une vulnérabilité. Plus une faille est facile à exploiter, plus la probabilité d'une attaque est élevée.

Le **risque** est le résultat de la combinaison entre une vulnérabilité, une menace, et la probabilité d'exploitation, menant à un préjudice.

2. Illustrer votre explication avec un exemple concret lié à une **injection SQL**, en tenant compte du fait que vous devez concevoir un site web ou une application.

L'injection SQL : est une attaque qui exploite une faille dans une application pour injecter du code SQL malveillant, permettant d'accéder, modifier ou supprimer des données dans une base de données.

Exemple d'une requête ordinaire:

```
SELECT * FROM utilisateurs WHERE username='$input' AND password='$password';
```

Un attaquant peut entrer :

```
'OR 1=1--
```

Ce qui transforme la requête en:

```
SELECT * FROM utilisateurs WHERE username='' OR 1=1--' AND password='';
```

Cela donne accès à tous les comptes.

Illustrer votre explication avec une exemple concret lié à une **injection SQL :**

- **Vulnérabilité**: Formulaire acceptant des entrées utilisateur sans filtrage ni requêtes préparées.
- **Menace** : Un attaquant tente d'exploiter cette faille pour accéder aux données.
- **Attaque**: L'attaquant injecte du code SQL (`'OR 1=1--`) pour contourner l'authentification.
- **Préjudice**: Vol ou suppression de données, compromission des comptes utilisateurs.
- **Probabilité**: Élevée si aucune protection n'est mise en place.
- **Risque**: Critique si l'application contient des données sensibles et qu'aucune mesure de sécurité n'est appliquée.

3. **Calcul :** Si la probabilité d'une attaque est de 30 % et que le préjudice potentiel est estimé à 100 000 €, quel est le risque associé ? Utilisez la formule d'estimation du risque.

Formule: Lerisque=préjudice*Probabilitédeproduction

Données:

Probabilitéd'attaque= 30 % =0.30

Préjudice potentiel=100 000 €

Calcul:

Risque = 0.30 × 100000 €

Risque = 30000 €

Interprétation:

Le risque estiméest 30 000 €. Cela signifie qu'en moyenne, l'impact financier attendu de cette attaque est de30000€,cequijustifielamiseenplacedemesuresdesécuritépourréduiresoitlaprobabilitéd'attaque,soitle préjudice potentiel.

Question4 : Politiquesdesécurité

1. Qu'est-cequ'unepolitiquedesécuritéetquelssontsesobjectifs?

(Def dans le cours: Une politique de sécurité est un ensemble de règles, de procédures et de bonnespratiquesmisesenplacepourprotégerlessystèmesinformatiques,lesdonnéesetlesutilisateurscontre les menaces et les risques de sécurité

Objectifs:Disponibilité,Confidentialité,Intégrité,Authentification,Traçabilité,Non-répudiation)

2. Associezchaquescénarioci-dessousàl'objectifde sécuritéqu'ilcompromet:
   a. Unserveurtombeenpanne,rendantlesdonnéesinaccessiblespendantplusieursheures (Disponibilité)
   b. Un acteur malveillant accède à une base de donnéesclient en exploitant une faille de sécurité (Confidentialité)
   c. Unvirusaltèredes fichierscritiquessurunserveur(Intégrité)
   d. Unthreatactorutiliselesidentifiantsvolésd'unemployépouraccéderauréseaudel'entreprise (Authentification)
   e. Une transaction financière est effectuée,mais aucun enregistrement de l'utilisateur ne peut en attester (Traçabilité)
   f. Unclientnieavoirpasséunecommandeenligne,alorsquelesystèmeprouvelecontraire (Non-répudiation)
   g. Unfichierconfidentielestmodifiéentransitparunattaquant(Confidentialitéet Intégrité)
   h. Unepannedeserveurentraîneunepertededonnées,etilestimpossibled'enidentifierlacause exacte (Disponibilité et Traçabilité)
3. Quelle est la différence entre un pare-feu (Firewall), un système de détection d'intrusion (IDS) et un système de prévention d'intrusion (IPS) dans la mise en œuvre d'une politique de sécurité ?

   Pare-feu(Firewall):Filtreletraficréseauenappliquantdesrèglesdesécuritépourautoriseroubloquer les connexions. Il agit comme une barrière entre un réseau sécurisé et un réseau nonfiable.

Système de détection d'intrusion (IDS) : Surveille les logs (réseau, système, ..) qui dépasse leFirewalletdétectelesactivitéssuspectesoumalveillantes,maisiln'intervientpasdirectementpour bloquer les attaques.

Système de prévention d'intrusion (IPS) : Fonctionne comme un IDS, mais avec la capacité debloquer ou neutraliser automatiquement les menaces détectées en temps réel.

Question5: Attaquesetcontre-mesures

1. Quelleestladifférenceentreuneattaquepassiveetuneattaqueactive? Donnezunexemplepour chaque type.

Attaquepassive :L'attaquantespionnelescommunicationsoucollectedesinformationssansmodifierlesdonnées ni perturber le système. L'objectif est la surveillance ou l'exfiltration d'informations.
Exemple :L'écoute clandestined'untraficréseau(sniffing)pourcapturerdesidentifiantsde connexion.

Attaqueactive:L'attaquantmodifie,altèreouinterromptlescommunicationsoulesdonnéespourcauserdes dommages ou obtenir un avantage.
Exemple :UneinjectionSQLpermettantàunattaquantdemodifierousupprimerdesdonnéesd'une base.

2. Complétez le tableau suivant en associant chaque type d'attaque à sa catégorie, sa description et un exemple :

Type d'attaque	Catégorie	Description	Exemple
Interception	Passive	Dansle cours	Sniffing
Interruption	Active		ARPPoisoning
Modification	Active		Maninthemiddle(MiTM)
Fabrication	Active		DDoS

Question6: La normeISO 27000

1. Quelestl'objectifprincipaldelanormeISO27000?
2. Quellessontlesprincipalesnormesdelafamille ISO27000etquelestlerôledechaque norme?
3. Quellessontlesquatrephasesdela normeISO27000etquelestl'objectifdechaquephase.

Sécuritéinformatique

Série2 :Initiationàlacryptographie(César/ Transposition)

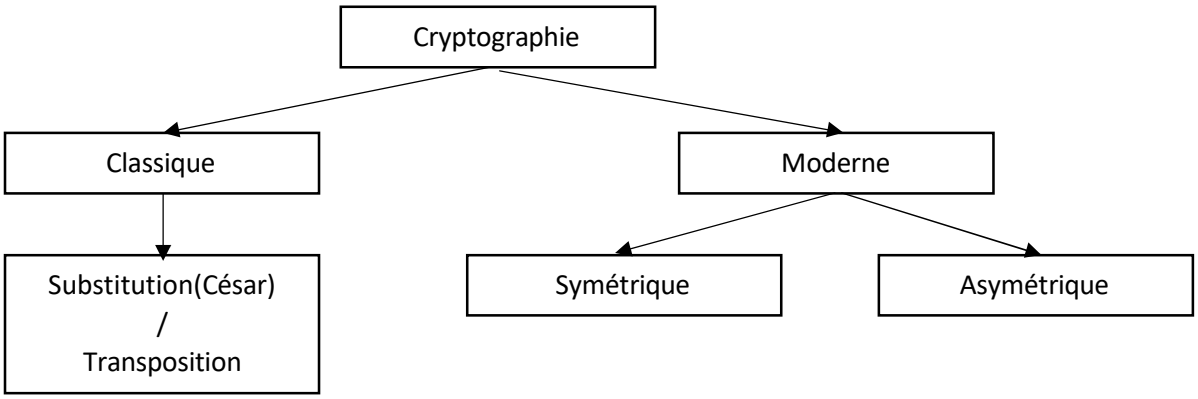
«*La cryptographie est l'art et la science de sécuriser les communications en transformant des informations en un format illisible pour toute personne non autorisée, puis en les rendant lisibles uniquement pour ceux qui possèdent la clé de déchiffrement appropriée.* »

1. ObjectifsdelaCryptographie?

2. PrincipauxConcepts:

- Chiffrement
- Déchiffrement
- Clé
- Algorithme
- Cryptanalyse

3. Typesde Cryptographie:



Exercice1:(Algorithmede César)

ChiffrementavecI'algorithmedeCésar

Chiffrezlemessagesuivantenutilisantl'algorithmedeCésaravecun décalagede3lettres: Message clair : "BONJOUR"

Déchiffrementavecl'algorithme de César

Déchiffrezlemessagesuivantquiaétéchiffréavecl'algorithmedeCésaravecundécalagede5lettres: Message chiffré : "GFION RTPMYFW"

DéchiffrementsanscléavecI'algorithmedeCésar

Déchiffrezlemessagesuivantquiaétéchiffréavecl'algorithmedeCésar sansconnaîtreledécalage: Message chiffré : "HUUHIH"

Exercice2:(Algorithmedechiffrementpartransposition)

Parexemple,enutilisantlaclé k=164325

LemessageclairM=«MESSAGESECRETACHIFFRERPARTRANSPOSITION»,

NousobtenantlecryptogrammeC=«METFRPOARIPNTSCHRAI SECERSGEFASIESARTON»

Chiffrement	Déchiffrement
1. Calculerlenombredecaractèresdumessage clair M. 2. Préparationdelamatrice: a. Colonnes(selon laclé) b. Lignes(Nb.M/ Nb.Cle) 3. Remplissagepar Lignes 4. Écrirele message parColonnesselonla clé	1. Calculerlenombredecaractèresdumessage Chiffré C. 2. Préparationdelamatrice: a. Colonnes(selonlaclé) -6- b. Lignes(Nb.M/ Nb.Cle)6+6+ … + 2 3. Remplirle message CparColonnesselonla clé 4. Écrirele messageMPar lignes

QuelestlecryptogrammeCcorrespondantautexteclairM=«MATHEMATIQUESETINFORMATIQUE » et la clé k = « 356124 » ?

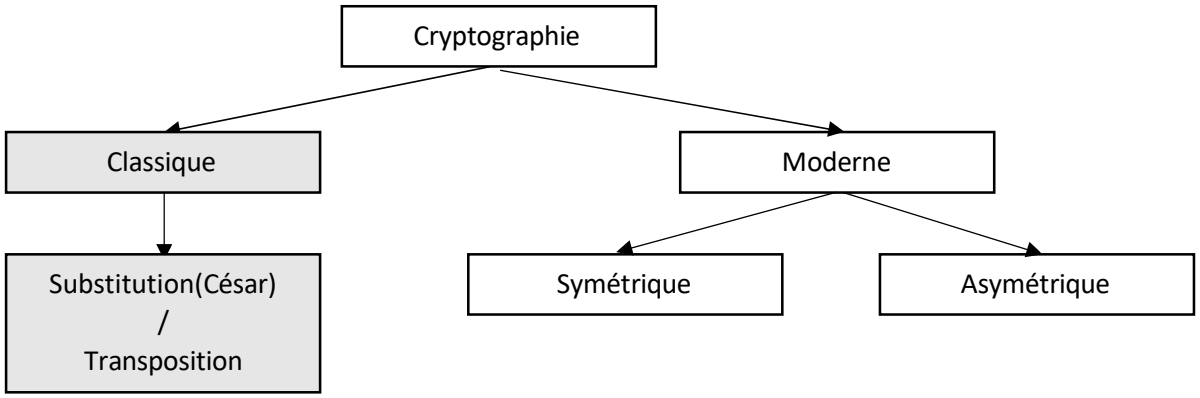
QuelestletexteclairMcorrespondantaucryptogrammeC«USCCLSETFEIESTCSEADEXCENA »et la clé k = « 356124 » ?

TDSécuritéInformatique

SérieTD3.1:*CryptographieSymétrique(S-DES)*

Rappel:

- Série1:Service,Menaces,Mécanismes,ISO 27002
- Série2:Cryptographieclassique(César,Transposition)



CryptographieSymétrique(S-DES):

1. Quelleestladifférenceentrelacryptographiesymétriqueetasymétrique?
2. Commentlesdeuxpartiescommunicantess'échangent-elleslaclésecrète danslecontextedela cryptographie symétrique afin de garantir la confidentialité des données échangées ?
3. Listedesalgorithmesdechiffrementsymétriquelesplusconnus:
   - AES(AdvancedEncryption Standard)
   - ~~DES(Data Encryption Standard)~~
   - 3DES(Triple Data Encryption Standard)

4. Quelleestla différence fondamentaleentrel'algorithme **S-DES**(SimplifiedDataEncryptionStandard)et le **DES** (Data Encryption Standard) complet ?

S-DESorSimplifiedDataEncryptionStandard

1. S-DESchiffredesblocsde**8 bits**.
2. La **clé**dechiffrementestde**10 bits**.
3. Deuxtoursdechiffrement.

Exemple:

TrouvezlesvaleursdeK1,K2,etletextechiffréenutilisantl'algorithmeS-DESaveclesparamètres suivants :

- Clé:10111 00111->K1: 1011 1110/ K2: 1101 1011
- Plaintext:01101100

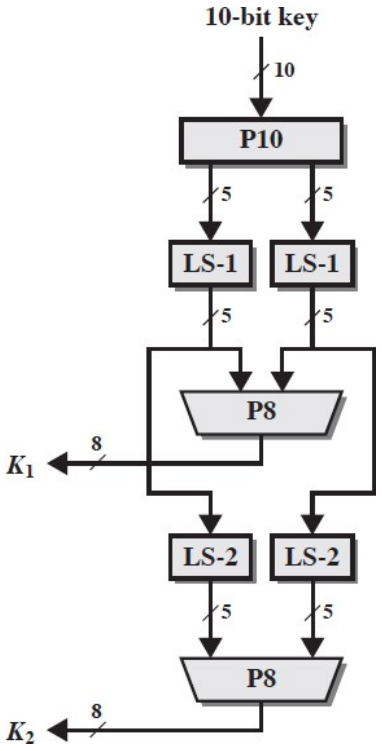
Exercise 01:

TrouvezlesvaleursdeK1,K2,etletextechiffréenutilisantl'algorithmeS-DESaveclesparamètres suivants :

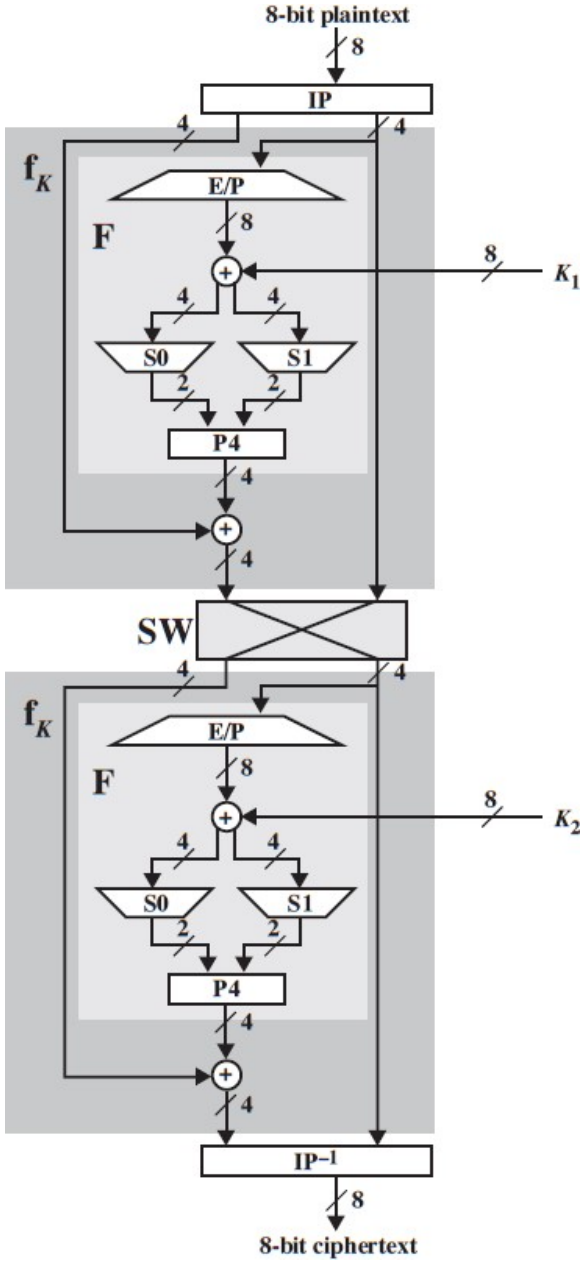
- Clé: 10100 00010
- TexteClair(r):01110010

Indiquezclairementvoscalculspourchaqueétape.

1. GénérationdesClés



2. Chiffrement



Permutations(inchangeable)

P10									
3	5	2	7	4	10	1	9	8	6

P8							
6	3	7	4	8	5	10	9

IP							
2	6	3	1	4	8	5	7

IP^{-1}							
4	1	3	5	7	2	8	6

E/P							
4	1	2	3	2	3	4	1

P4			
2	4	3	1

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

TDSécuritéInformatique

SérieTD3.2 :CryptographieAsymétrique(RSA)

Àvotreavis,quellessontles**limites**delacryptographiesymétrique?

Cryptographieasymétrique:L'algorithmeRSA

L'algorithme RSA est un algorithme de cryptographie asymétrique largement utilisé. RSA a été publié pour la premièrefoisen1977parRonRivest,AdiShamiretLeonard Adleman,d'oùsonnomRSA (Rivest-Shamir-Adleman).

1. Chaqueutilisateurpossèdedeuxclés:uneclépubliqueetunecléprivée.
2. Lacléprivéedoitêtrestockée demanière sécuriséeetnedoitjamaisêtre divulguéeàquiconque.
3. Ilestimpossibledededéduireunecléàpartir del'autre,carellessontgénéréesàl'aidedeformules mathématiques irréversibles.
4. Sivouschiffrezunmessageavecl'unedesclés,vouspouvezledéchiffreravecl'autreclécorrespondante.

RSA :ModedeFonctionnement

Phase1:Générationdesclés(publiqueet privée)

1. **Choisir deux nombres premiers distincts :** Choisissez deux nombres premiers distincts ***p*** et ***q***. Ces nombres doiventêtresuffisammentgrandspour assurerlasécuritédu système.Pluscesnombressontgrands,plusla sécurité est renforcée. *(P=3, Q=11)*

2. **Calculer*n*:**Calculezleproduitdesdeuxnombrespremiers:***n* =*p*× *q***.

3. **Calculerlafonctiond'Euler*φ*(*n*):**Calculer lafonctiond'Eulerde***n***, quiestlenombred'entierspositifsinférieurs à ***n*** qui sont premiers avec ***n***. Pour deux nombres premiers distincts ***p*** et ***q***, ***φ*(*n*)** =(*p*−1)×(*q*−1).

4. **Choisir*l'*exposantdechiffrementpublic(e):**Sélectionnezun entier***e*** telque**1<*e*<*φ*(*n*)**et***e***estpremieravec ***φ*(*n*)**.***e***estgénéralementchoisi petit.

5. **Calculerl'exposantdedéchiffrementprivé (*d*):** enutilisonsl'algorithmed'Euclideétendu,calculezl'exposantde déchiffrement ***d*** : ***d*×*e*≡1 mod *φ*(*n*)**

6. **Clésgénérées:**Lescléspubliquessont**(*n*,*e*)** etlacléprivéeest***d***.

Unefoisquevousavezgénérélesclés,vouspouvezutiliserlaclépubliquepourchiffrerles messagesetlacléprivée pour les déchiffrer.

Phase2:Chiffrementdumessage

Si**M**estun**entier**naturelstrictementinférieurà n représentantunmessage, alorslemessagechiffrésera représenté par : $\boxed{C = M^{e} \bmod (n)}$ *(prenons Exemple : M=4 -> C=31)*

Phase3:Déchiffrementdumessage

$\boxed{M=C^{d} \bmod (n)}$

Exercise01:

Alicesouhaiteenvoyerlemessage"Hello"àBobdemanièresécuriséeenutilisantRSA.Lesparamètresdechiffrement sont les suivants : p = 17, q = 11, e=7

- CalculezN,l'entierdemoduleRSA.
- Calculezϕ(N),lafonctiond'EulerdeN.
- Vérifiezqueeestpremieravecϕ(N).
- Trouvezl'exposantdedéchiffrementd.

1. Bobchoisitlemot"Hello"àenvoyer àAlice. UtilisezlecodeASCII pourtransformerleslettresen chiffresentiers, puis utilisez la clé publique (N, e) pour chiffrer le message.
2. Aliceutilisesaclé privéepourdéchiffrerle message.