

Sécurité

Dr. OMAR Mawloud

Maître de Conférences à l'Université A. Mira de Béjaia

PROGRAMME DU MODULE

- Chapitre 1 (20%)
Introduction à la Sécurité
- Chapitre 2 (30%)
Algorithmes de Chiffrement à Clés Publiques
- Chapitre 3 (25%)
Gestion des Clés Publiques : Cas de PKI
- Chapitre 4 (25%)
Gestion des Clés Symétriques : Cas de Kerberos

MODE D'ÉVALUATION

- Examen
- Contrôle Continu (8 séances de TD)
 - Présence physique \Rightarrow 02 pts
 - 1 présence \Rightarrow 0,25 pts
 - 1 absence \Rightarrow 0 pts
 - 5 absences justifiées ou 3 absences non-justifiées
 - Présence complète (participation) \Rightarrow 04 pts
 - Une note d'évaluation sur 0,5 pts est attribuée à chaque étudiant lors de chaque séance de TD
 - Interrogation(s) \Rightarrow 15 pts

Chapitre I

Introduction à la Sécurité

Menaces et scénarios d'attaques

Algorithmes de chiffrement

Concepts de base liés à l'arithmétique modulaire

QUOI ET POURQUOI ?

- Quel est l'intérêt de pirater ?
 - Curiosité
 - Concurrence commerciale ou pour l'argent
 - Se montrer intelligent et se distinguer des autres
 - Ça fait plaisir de causer le mal aux autres
 - Analyser les vulnérabilités pour les corriger
- Les différents axes de la sécurité informatique
 - Protection des droits d'auteurs
 - Protection contre les codes malveillants
 - Protection contre le spamming
 - **Protection des données dans les réseaux de communication**

LOGICIELS ET DROITS D'AUTEURS

- Comment protéger son logiciel ?
 - Protection à l'aide d'un numéro de série
 - Protection à l'aide d'un support physique
- Que veut dire pirater un logiciel ?
 - Dériver une autre version qui fonctionne sans protection
- Comment pirater un logiciel ?
 - Le meilleur moyen c'est d'avoir un « décompilateur »
 - Fichier exécutable \Rightarrow Code source en C++
 - Fichier exécutable \Rightarrow Code source en Java
 - On peut utiliser le désassembleur

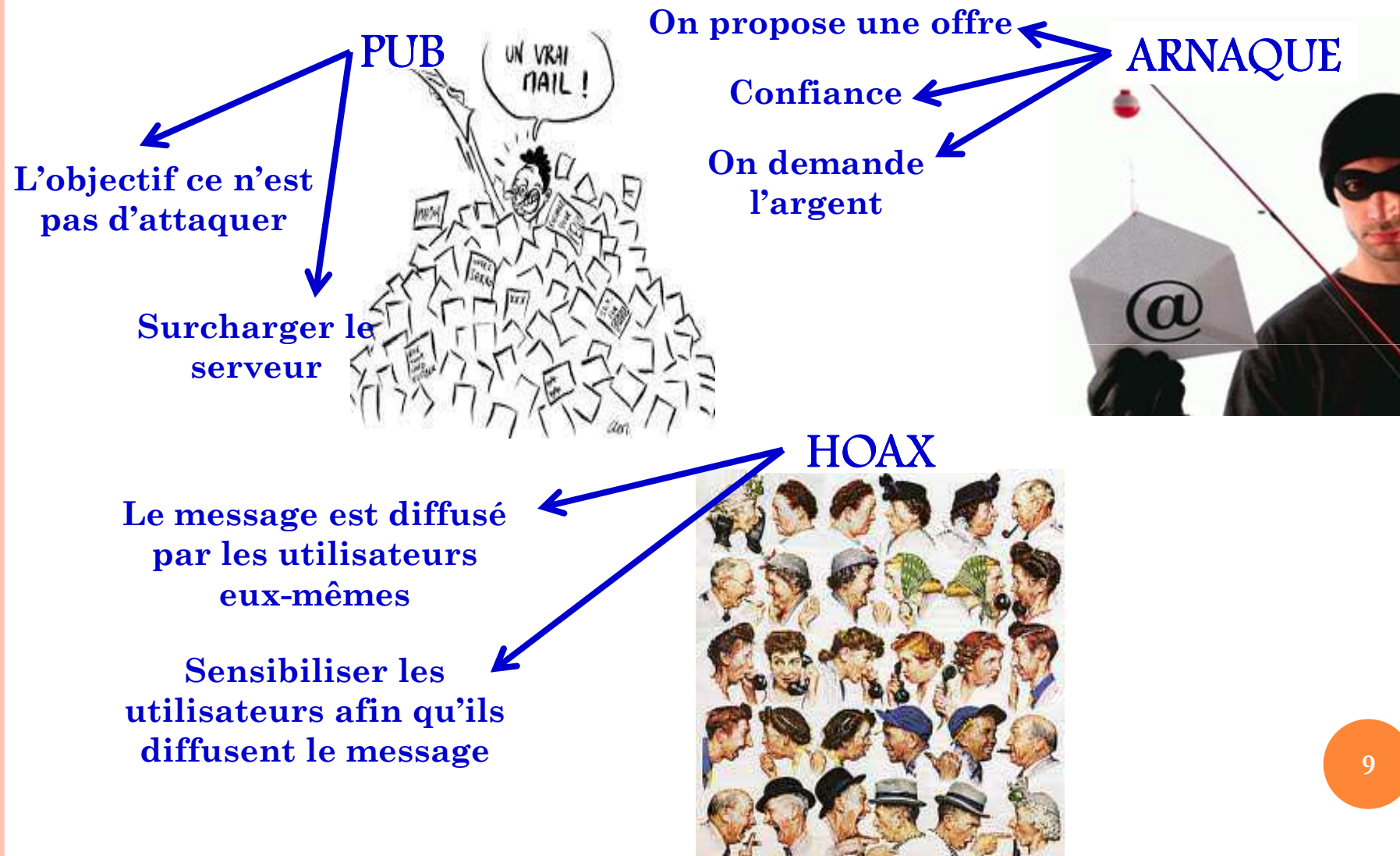
LOGICIELS ET DROITS D'AUTEURS

- Désassembleur
 - Permet d'afficher le programme en assembleur (WinDasm)
- Editeur hexadécimal
 - Permet de modifier le fichier exécutable (WinHex)
- Comment enlever la protection ?
 - 1) Lancer l'exécutable et taper un numéro de série aléatoire et retenir le message d'erreur
 - 2) Désassembler le fichier exécutable
 - 3) Chercher le texte du message d'erreur dans le programme
 - 4) Repérer l'instruction qui effectue un test avant d'afficher le message d'erreur
 - 5) Inverser la condition en utilisant l'éditeur hexadécimal

LES CODES MALVEILLANTS

- Programme malveillant capable d'infecter un autre en le modifiant de façon à ce qu'il puisse à son tour se reproduire
- ⇒ Virus informatique
- Programme malveillant caché dans un autre qui donne accès à la machine victime sur laquelle il est exécuté et sur laquelle il exécute des commandes à distance
- ⇒ Cheval de Troie (Trojans)
- Programme malveillant dupliqué sur plusieurs machines dont le déclenchement s'effectue à un moment déterminé pour attaquer une machine victime
- ⇒ Bombes logiques (DoS – Denial of Service)
- Programme malveillant qui collecte des informations de la machine sur laquelle il est exécuté et de les envoyer
- ⇒ Espiogiciels (Spywares)

LE SPAMMING



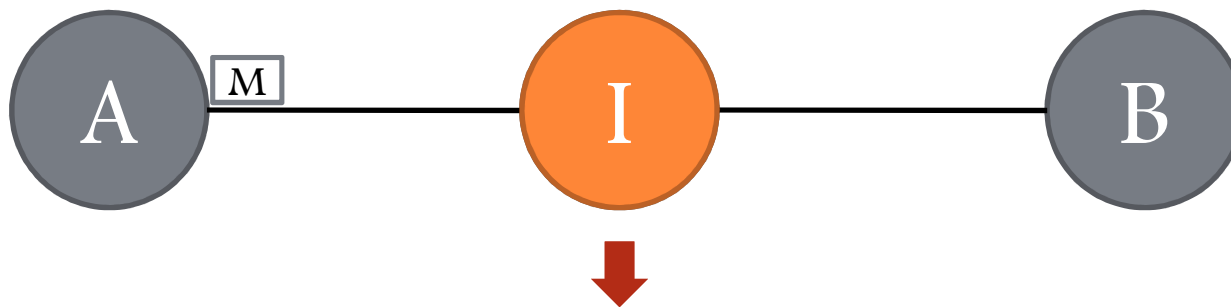
LES HOAX

Je vous envoie ce truc parce que c'est trop surprenant, mon vœu s'est réalisé !! J'espère que ça te fera plaisir : 20min après avoir fait ça, mon vœu s'est produit. La personne qui me l'a envoyé m'a dit que son vœu avait fonctionné 15 min après avoir lu le message. Le hasard n'existe pas ! Essaie-le pour voir ! Fais un vœu avant que le comptage ne soit fini !! Commence à descendre après avoir formé ton vœu : 10 ... 9 ... 8... 7 ... 6 ... 5 ... 4 ... 3 ... 2 ... 1. Fais un vœu ! Envoie cet email à 10 personnes avant une heure. Si tu fais, ton vœu se réalisera. Si tu ne le fais pas, le contraire de ton vœu va se produire! Bonne chance. Condition d'utilisation le renvoyer au plus grand nombre de personnes. Recopies le message et colle-le dans un nouveau : Al Qayum, Al Majid, Al Wajid, Al Wahid, Al Ahad, Al Samad, Al Quadir, Al Malik, Al Rahman, Al Rahim. Allah n' échoue jamais. Envoyez ce message à neuf personnes, vous obtiendrez de bonnes nouvelles demain. Si vous le négligez, mauvaise chance pendant neuf années. C'est vérité prouvée. Ne prenez pas le risque. Seulement envoyer à neuf messages au nom d'Allah

LES ARNAQUES

Excusez-moi pour cette intrusion, je suis CORINNE BURIERE d'origine française et cela fait deux 2 jours que J'ai contacté une association qui s'occupe des enfants démunis et pas de réponse. Mais j'ai pu me mettre en contact avec vous ceci grâce à la volonté de DIEU. Cela fait quelques mois que j'ai été atteint d'un cancer en phase terminale détectée trop tard et selon les dires de mon médecin, je n'ai plus assez de temps à vivre. En ce moment je suis hospitalisée dans un hôpital à Londres. J'ai toujours privilégié le service de ma nation au détriment de ma propre santé et voilà aujourd'hui cela me rattrape, mais je suis fière d'avoir pu aider des gens autour de moi et je pense pouvoir continuer à le faire à travers vous. J'ai Perdu mon mari et mes deux enfants dans un crash d'avion qui s'était produit à New York. J'aimerais que vous soyez le bénéficiaire de toute ma fortune qui est d'une somme exactement chiffrée à 1.500.000 euros que vous utiliserez pour aider les enfants pauvres et déshérités vu que mes jours sont comptés. Aussi, ce matin j'ai reçu un message de ma banque me disant que l'État aimerait récupérer mes fonds après ma mort vu que je n'ai pas d'héritier(e). Veuillez m'aider en acceptant mon offre. Répondez-moi vite. Que le Seigneur vous garde.

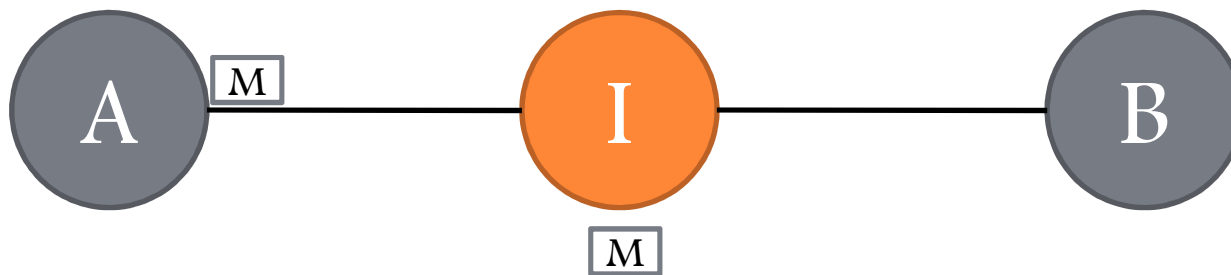
PROTECTION DES DONNÉES DANS LES RÉSEAUX DE COMMUNICATION



- Routeur dans un réseau filaire
- Point d'accès dans un réseau mobile
- Machine intermédiaire dans un réseau mobile ad hoc

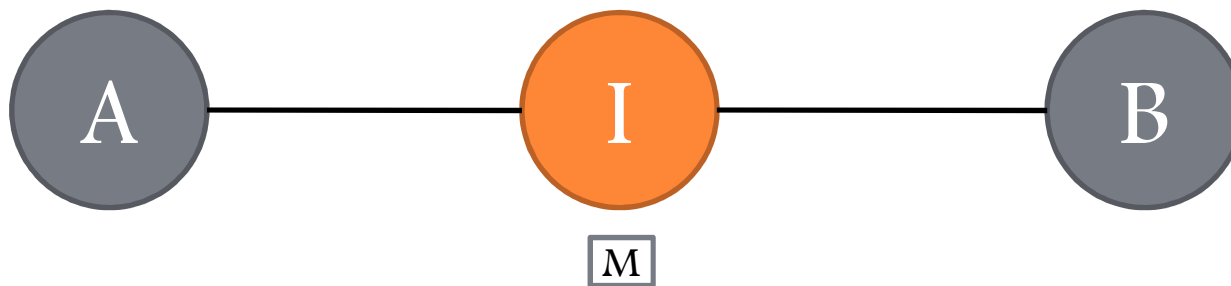
Attaquant Potentiel

L'INTERCEPTION



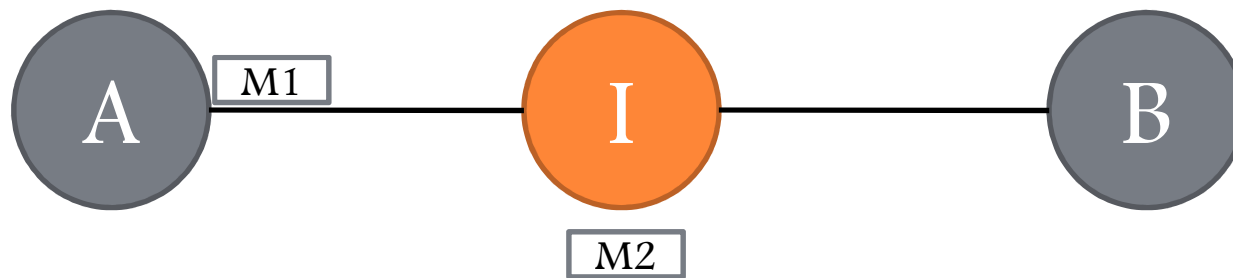
La confidentialité

LA FABRICATION



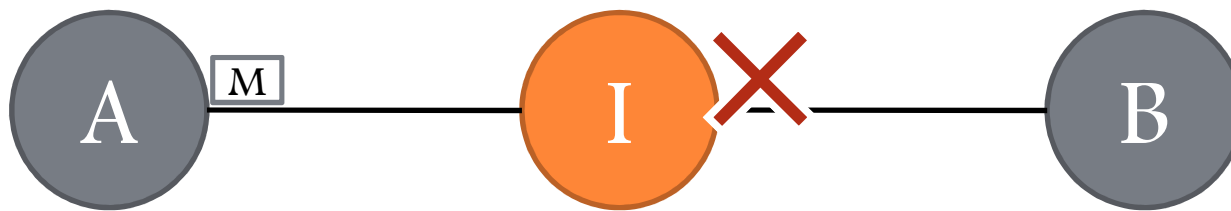
L'authentification

LA MODIFICATION



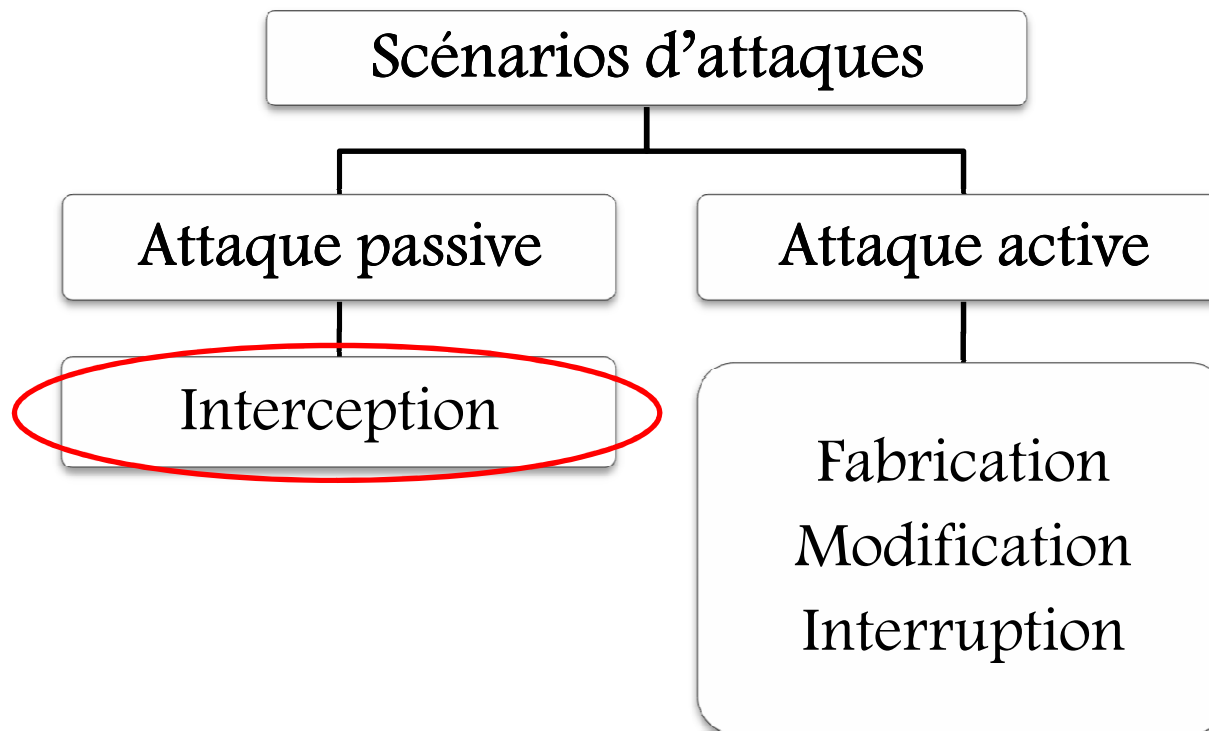
L'intégrité

L'INTERRUPTION



Disponibilité

LES SCÉNARIOS D'ATTAQUES

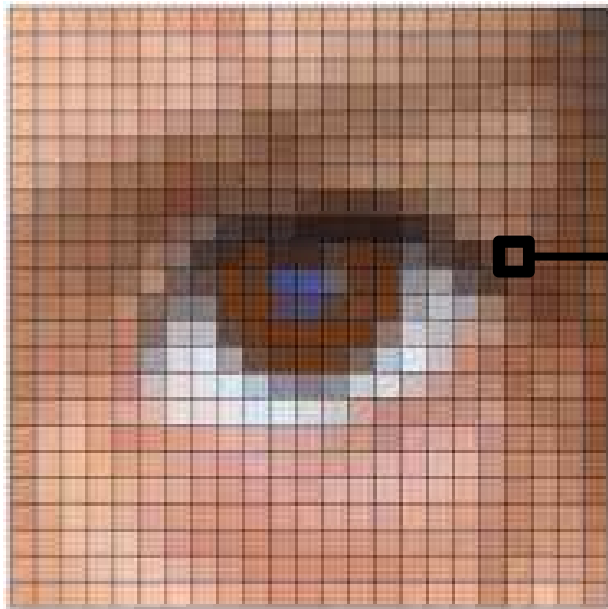


LA STÉGANOGRAPHIE

- Dissimuler un secret dans un support anodin
- Stéganographie classique
 - Dissimuler un message secret dans un autre message
 - Exemple : Collecter les mots de positions impaires
 - Il ne faut pas tuer Jules César car il n'est pas le vrai coupable
 - Il ne faut pas tuer Jules César car il n'est pas le vrai coupable
 - Il faut tuer César il est le coupable
- Stéganographie moderne
 - Les trames ⇒ Exploiter les champs non-utilisés
 - Les exécutables ⇒ Déclaration des variables strings inutiles
 - Images ⇒ Exploiter les bits de poids faibles du pixel

LA STÉGANOGRAPHIE MODERNE

- Chaque pixel d'une image (format bmp) est représenté par 3 nombres codés sur 8 bits
 - R \Rightarrow l'intensité du rouge
 - G \Rightarrow l'intensité du vert
 - B \Rightarrow l'intensité du bleu



R = 122
G = 126
B = 127

LA STÉGANOGRAPHIE MODERNE

- Image composée de deux pixels
 - $R_1 = 01001110$ $G_1 = 01101111$ $B_1 = 11111111$
 - $R_2 = 01110011$ $G_2 = 01110110$ $B_2 = 10101010$
 - $M = 101100011011$
 - $R_1 = 01001110$ $G_1 = 01101111$ $B_1 = 11111100$
 - $R_2 = 01110001$ $G_2 = 01110110$ $B_2 = 10101011$
- Très discret
- Permet de cacher des messages de tailles importantes
 - Image $40 \times 40 \Rightarrow 40 \times 40 \times 6 = 9600$ bits $\Rightarrow 1200$ caractères
- Il faut transmettre les fichiers en format bmp
- Toute compression fait perdre le message caché

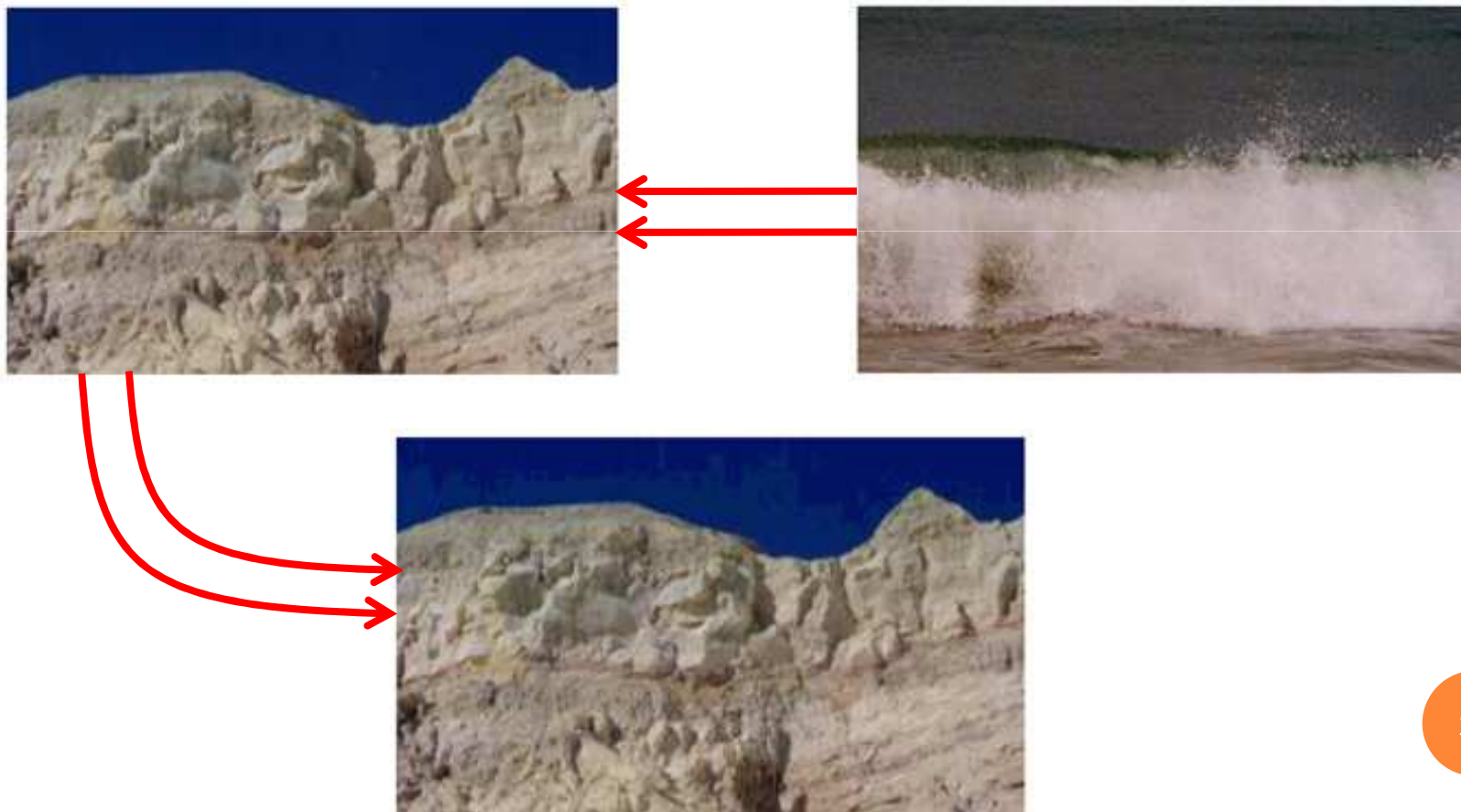
LA STÉGANOGRAPHIE MODERNE

- Exemple 1 : Message caché dans une image

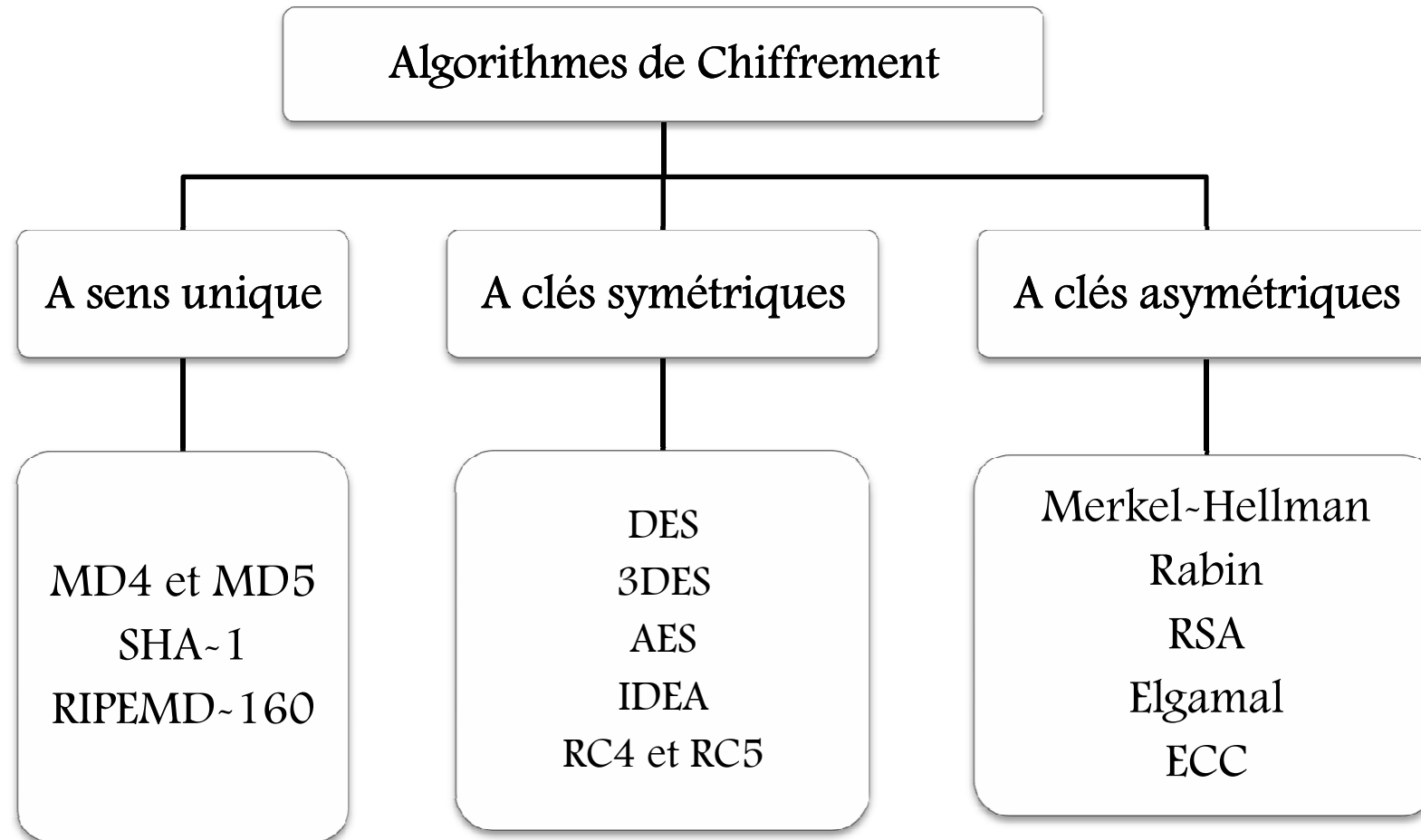


LA STÉGANOGRAPHIE MODERNE

- Exemple 2 : Image cachée dans une image



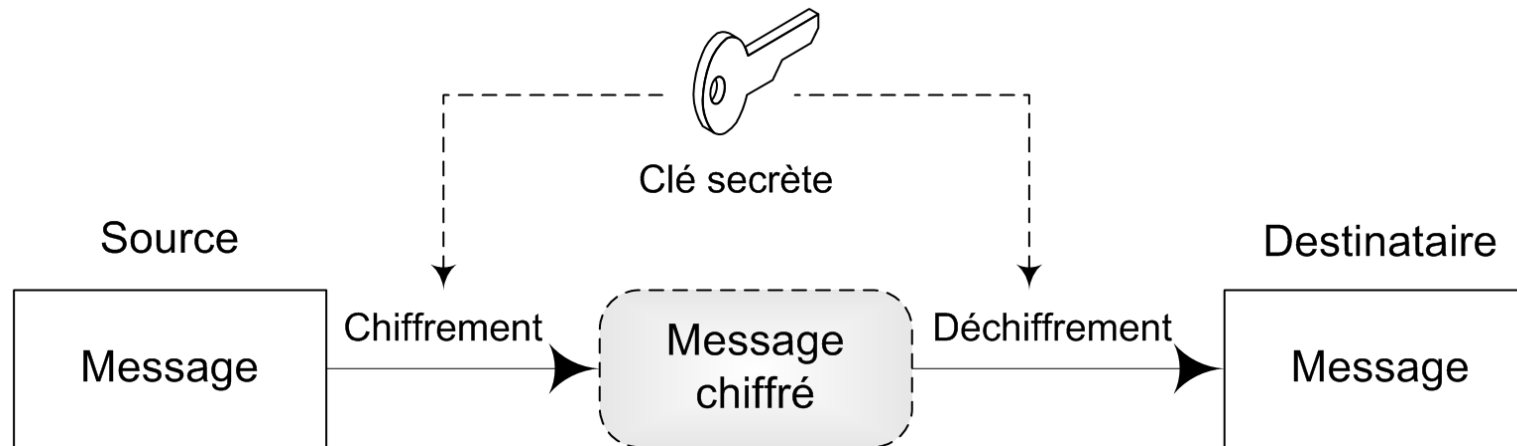
CHIFFREMENT MODERNE



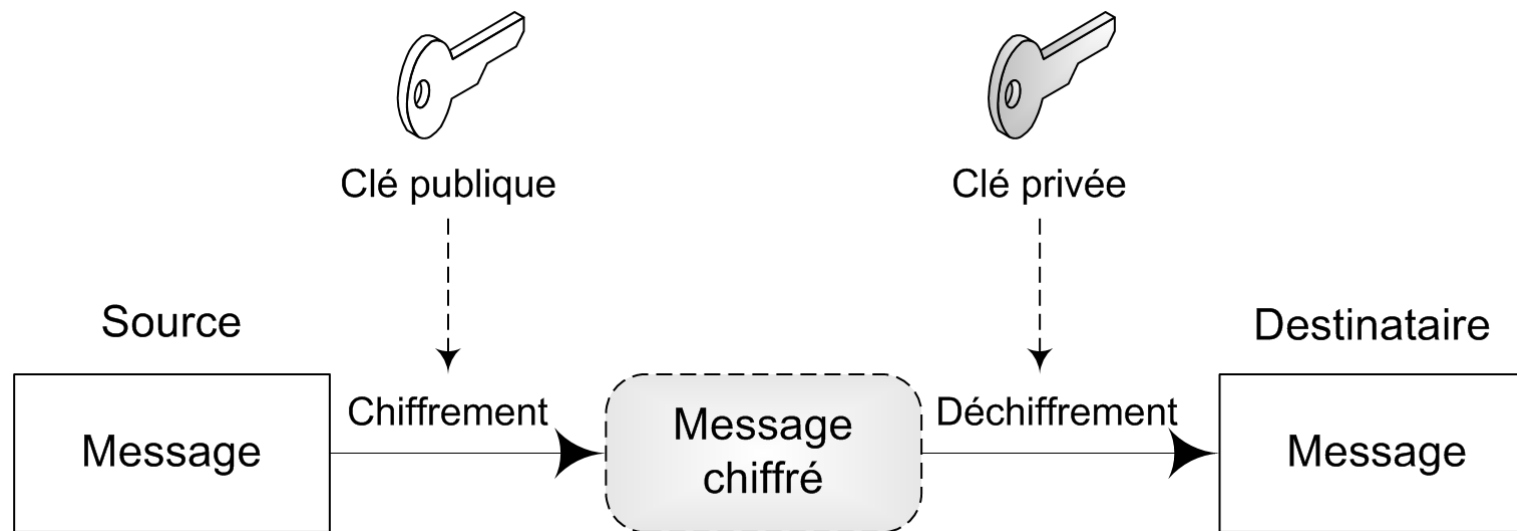
CHIFFREMENT À SENS UNIQUE

- $h=H(M)$
- La valeur de h est de longueur fixe et inférieure à M
- A partir de h , il est impossible de retrouver M
- Il est difficile de trouver M' tel que $H(M')=h$

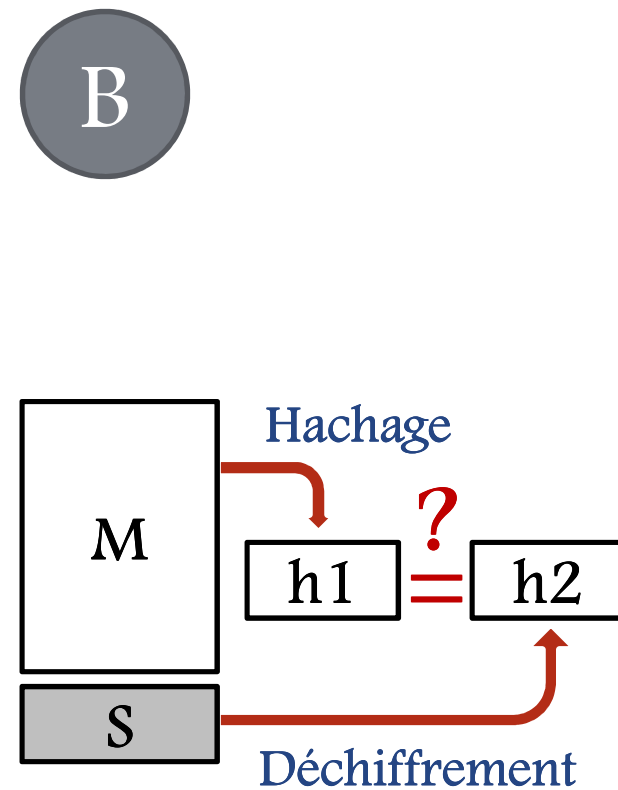
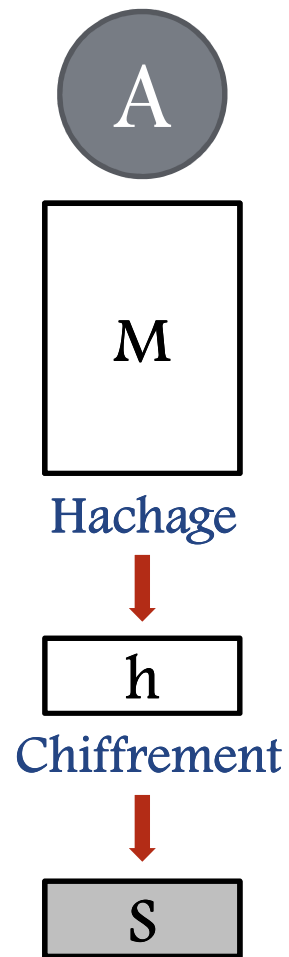
CHIFFREMENT À CLÉS SYMÉTRIQUES



CHIFFREMENT À CLÉS ASYMÉTRIQUES



SIGNATURE NUMÉRIQUE



SYMÉTRIQUE OU ASYMÉTRIQUE ?

- Une clé publique RSA de 512 bits :

524316579815732615978461375
164524134612451697857631957
251623797185462312546294826
789456312549567312596976481
e.6754891637215697854631254
C = M mod n 49264321594957306 78496
498157575778 2564
7623156 46756132
24519515463565
3426158926552115207

Charge de calcul

SYMÉTRIQUE OU ASYMÉTRIQUE ?

- Soit une clé publique RSA de 512 bits, tel que $n =$

109417386415705274218097073220403576120037329454492059909138
421314763499842889347847179972578912673324976257528997818337
97076537244027146743531593354333897 =

102639592829741105772054196573991675900716567808038066803341
933521790711307779

\times 1066034883801684548209272203600128786792079585759892915222
70608237193062808643

- Institut National de Recherche en Informatique et en Science Informatique d'Algérie

- 300 ordinateurs et 25 jours de calcul !!

ALGORITHME D'EXPONENTIATION RAPIDE

- $C = B^A \bmod N$
- A partir du triplet (P, J, R) / $P=B, J=A$, et $R=1$
- Si J est pair $\Rightarrow (P^2 \bmod N, J/2, R \bmod N)$
- Si J est impair $\Rightarrow (P^2 \bmod N, (J-1)/2, R \times P \bmod N)$
- Si $J=1 \Rightarrow C=R \times P \bmod N$

- Exercice (5 mnt) : Calculer $C=150^{233} \bmod 437$

ALGORITHME D'EXPONENTIATION RAPIDE

- $C = 150^{233} \bmod 437$

- A partir de $(P=150, J=233, R=1)$

$$\rightarrow (150^2 \bmod 437, (233-1)/2, 1 \times 150 \bmod 437) = (213, 116, 150)$$

$$\rightarrow (213^2 \bmod 437, 116/2, 150 \bmod 437) = (358, 58, 150)$$

$$\rightarrow (358^2 \bmod 437, 58/2, 150 \bmod 437) = (123, 29, 150)$$

$$\rightarrow (123^2 \bmod 437, (29-1)/2, 150 \times 123 \bmod 437) = (271, 14, 96)$$

$$\rightarrow (271^2 \bmod 437, 14/2, 96 \bmod 437) = (25, 7, 96)$$


$$\rightarrow (25^2 \bmod 437, (7-1)/2, 96 \times 25 \bmod 437) = (188, 3, 215)$$

$$\rightarrow (188^2 \bmod 437, (3-1)/2, 215 \times 188 \bmod 437) = (384, 1, 216)$$

$$\rightarrow C = 384 \times 216 \bmod 437 = 351$$

ALGORITHME D'EXPONENTIATION RAPIDE

- $C = 150^{233} \bmod 437$
- $233 = 11101001_{(2)}$



1	150
0	$150^2 \bmod 437 = 213$
0	$213^2 \bmod 437 = 358$
1	$358^2 \bmod 437 = 123$
0	$123^2 \bmod 437 = 271$
1	$271^2 \bmod 437 = 25$
1	$25^2 \bmod 437 = 188$
1	$188^2 \bmod 437 = 384$

$$150 \times 123 \times 25 \times 188 \times 384 \bmod 437 = 351$$

ALGORITHME D'EUCLIDE ETENDU (LES ÉQUATIONS DIOPHANTIENNES)

- $396X + 17Y = 1$

- $396 = 23 \times 17 + 5$

$$17 = 3 \times 5 + 2$$

$$5 = 2 \times 2 + 1$$

- $1 = 5 - 2 \times 2$

$$= 5 - 2 \times (17 - 3 \times 5)$$

$$= 5 - 2 \times 17 + 6 \times 5$$

$$= 7 \times 5 - 2 \times 17$$

$$= 7 \times (396 - 23 \times 17) - 2 \times 17$$

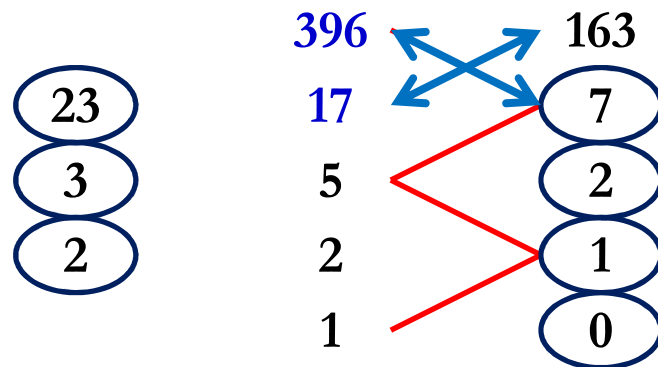
$$= 7 \times 396 - 161 \times 17 - 2 \times 17$$

$$= 7 \times 396 - 163 \times 17$$

$$= 396 \times 7 + 17 \times (-163) \Rightarrow \{X=7, Y=-163\}$$

ALGORITHME D'EUCLIDE ETENDU (LES ÉQUATIONS DIOPHANTIENNES)

$$396X + 17Y = 1$$



$$396 \times 7 - 17 \times 163 = 1 \quad \Rightarrow \quad \{X=7, Y=-163\}$$

Chapitre II

Algorithmes de Chiffrement à Clés Publiques

Protocole Diffie–Hellman

Chiffrement de RSA

Chiffrement de Rabin

Chiffrement de Merkle–Hellman

Chiffrement de ElGamal

PROTOCOLE DE DIFFIE~HELLMAN

- Inventé par Whitfield Diffie et Martin Hellman en 1976



Whitfield Diffie

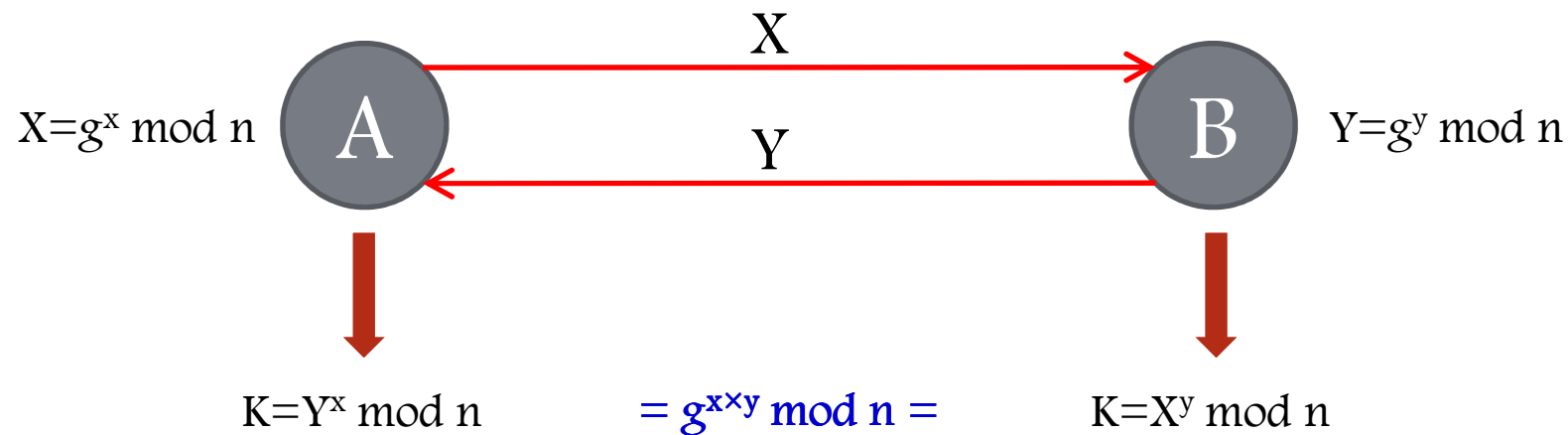


Martin Hellman

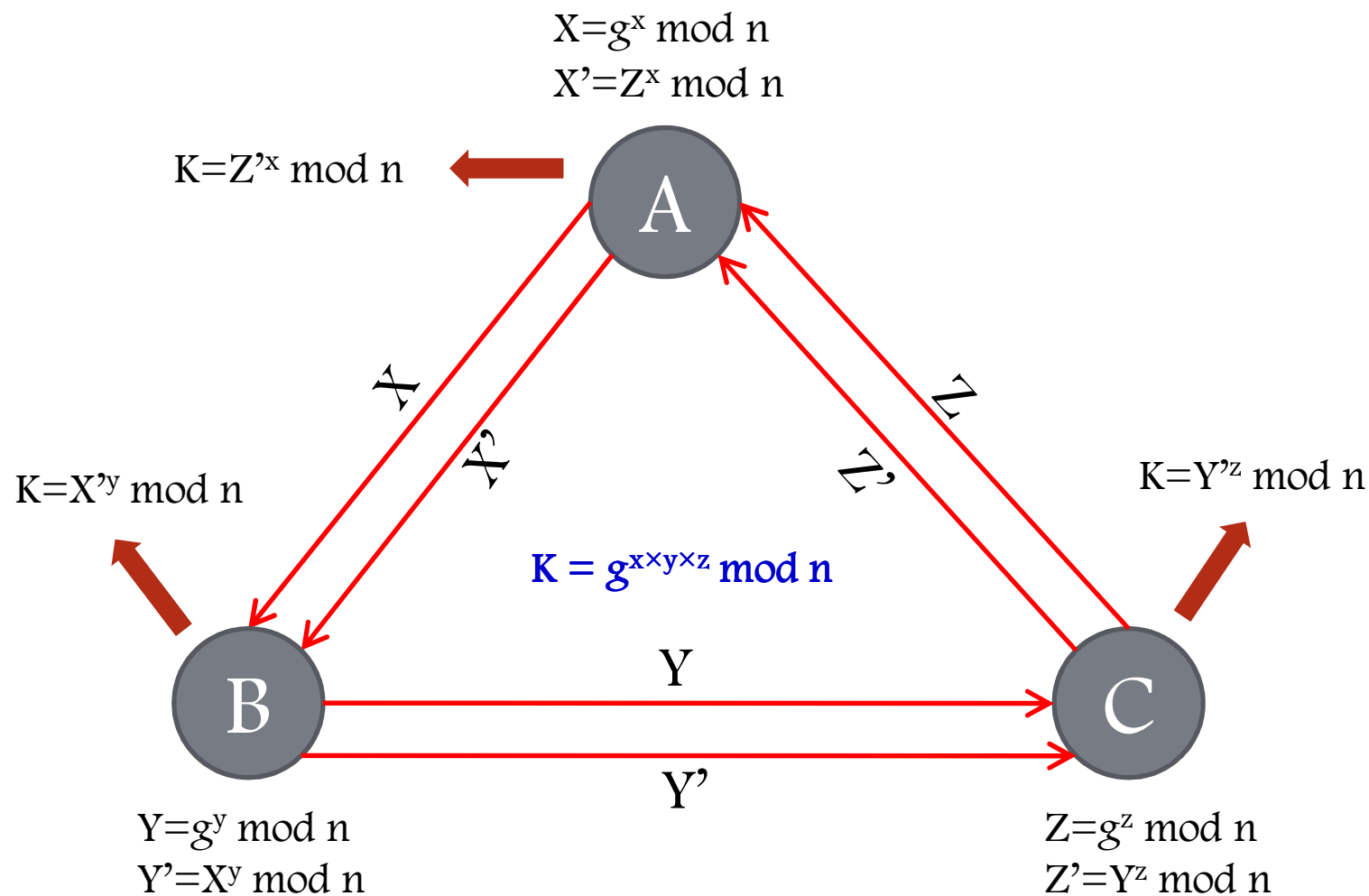
- La naissance de la cryptographie à clés asymétriques
- Partage d'une clé secrète par l'intermédiaire d'un échange de données publiques pouvant être interceptées
- Problème du Logarithme Discret $\Rightarrow A=B^x \bmod C$

PROTOCOLE DE DIFFIE~HELLMAN

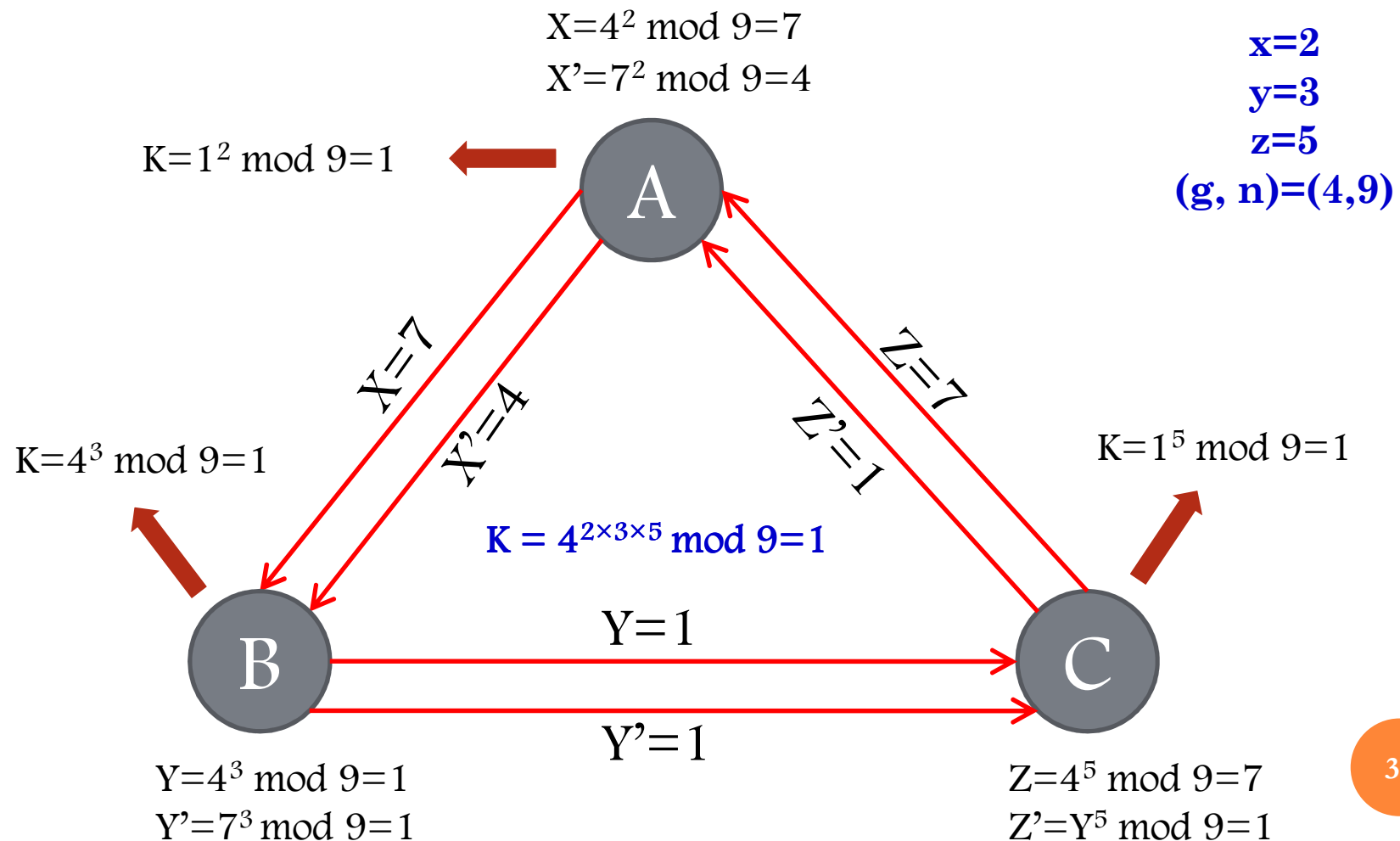
- A et B partagent deux paramètres $(g, n) \Rightarrow$ publique
- Clé privée de A $\Rightarrow x$
- Clé privée de B $\Rightarrow y$
- L'intrus intercepte $X = g^x \bmod n$?!



PROTOCOLE DE DIFFIE~HELLMAN



PROTOCOLE DE DIFFIE~HELLMAN



CHIFFREMENT DE RSA

- Inventé par Ron Rivest, Adi Shamir et Leonard Adleman en 1977



Ronald Rivest



Adi Shamir



Leonard Adleman

- Le premier système de chiffrement à clés asymétriques
- Problème de factorisation

CHIFFREMENT DE RSA

- Choisir deux grands nombre premiers p et q :
- Calculer $n=p \times q$
- Calculer $\varphi(n)=(p-1) \times (q-1)$
- Choisir $e < \varphi(n)$ tel que $\text{pgcd}(e, \varphi(n))=1$
- Calculer d tel que $e \times d \bmod \varphi(n)=1$
- Clé publique $\Rightarrow (e, n)$
- Clé privée $\Rightarrow (d, n)$
- Chiffrement $\Rightarrow C=M^e \bmod n$
- Déchiffrement $\Rightarrow M=C^d \bmod n$

CHIFFREMENT DE RSA

- Exercice (10 mnt) : $p = 19, q = 23, e = 17, M = 351$
- $n = 19 \times 23 = 437$
- $\varphi(n) = (19 - 1) \times (23 - 1) = 396$
- $17 \times d \bmod 396 = 1 \Rightarrow d = 233$
- $C = 351^{17} \bmod 437 = 150$
- $M = 150^{233} \bmod 437 = 351$