République Algérienne Démocratique Et Populaire
Ministère De L'enseignement Supérieur Et De La Recherche Scientifique
ECOLE NATIONALE POLYTECHNIQUE D'ORAN MAURICE AUDIN

Département Mathématiques et Informatique
Filière IMSI : 4ème année ingénieur

Sécurité des systèmes d'information

DR F.KABLI

kablifatima47@gmail.com

La cryptographie et ses applications : Algorithmes

Algorithme RSA :

- Algorithme de cryptage à clé publique.
- Développé par **R**ivest, **S**hamir et **A**delman en 1977

Les étapes de RSA :

1. Choisir deux nombres premiers p et q .
2. Calculer $n = p.q$ et son indicateur d'Euclide $\Phi(n) = (p-1).(q-1)$.
3. Choisir un nombre e premier avec $\Phi(n)$ (tel que $pgcd(e, \Phi(n))=1$).
4. La clé publique sera formée par **(e,n)**. On choisira ensuite un **d** tel que :

$$e.d = 1[\Phi(n)]$$

5. La clé privée sera donnée par (d,n).

La cryptographie et ses applications

Algorithme RSA :

- Le chiffrement par RSA :

Le chiffrement d'un message **M** en un message codé **C** se fait suivant la transformation suivante :

$$C = M^e \bmod n$$

- Le Déchiffrement par RSA :

Calculer la fonction réciproque

$$M = C^d \bmod n$$

La cryptographie et ses applications

Algorithme Diffie-Hellman

- Algorithme de partage de clé secrète entre deux entités.
- Développer par whitfield Diffie et Martin Hellman, Publiée en 1976.
- Deux utilisateurs peuvent se mettre d'accord sur un nombre pour chiffrer la conversation entre eux.

La cryptographie et ses applications

Algorithme Diffie–Hellman

Les étapes de D–H :

1. Les deux utilisateurs X et Y ont choisi un nombre premier P et un générateur g.
2. X choisit un nombre secret a
3. X envoie à Y la valeur $A = g^a \ [mod]\ P$
4. Y choisit un nombre secret *b*
5. Y envoie à X la valeur $B = g^b \ [mod]\ P$
6. X peut maintenant calculer la clé secrète : $B^a \ [mod]\ P$
7. Y fait de même et obtient la même clé que X : $A^b \ [mod\ ]p]$

La cryptographie et ses applications

Algorithmes

- DES (Data Encryption Standard)
- Triple D.E.S
- AES (Advanced Encryption Standard)
- RC4 (Rivest Cipher 4)
- ETC….

La cryptographie et ses applications

Cracker un mot de passe : Comment cracker des mots de passe enregistrés
dans des systèmes informatique:

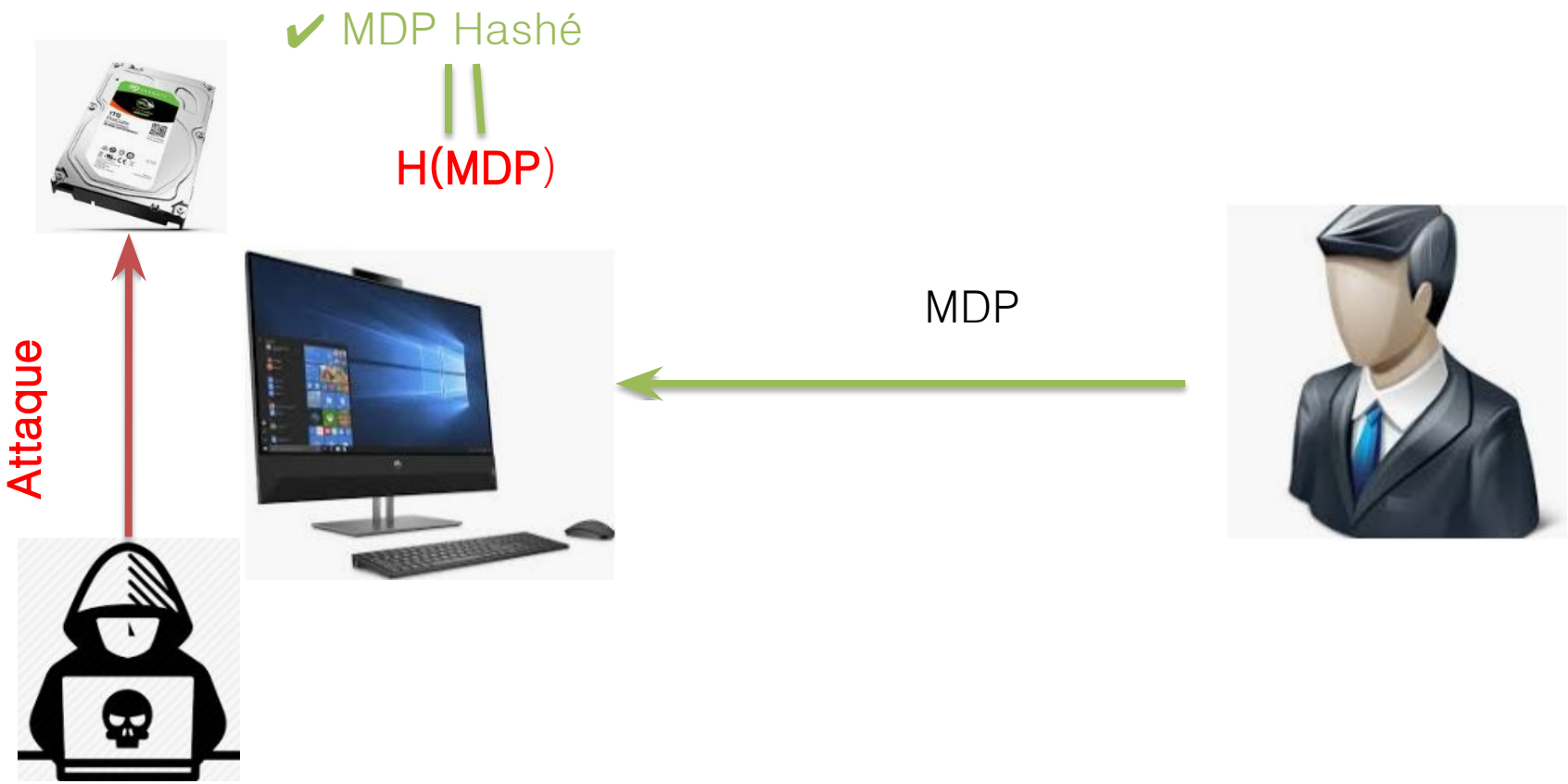
✔ MPD valide
✔MDP non valide

MDP

Attaque

La cryptographie et ses applications

Fonction de Hachage



La cryptographie et ses applications : Algorithmes

Cracker un mot de passe : Récupérer le mot de passe a partir du hash

- ❑ Accéder a la base de données.
- ❑ Récupérer les empreintes.
- ❑ Choisir une technique pour cracker le mot de passe

Les techniques :

- ✔ Attaque par force brute
- ✔ Attaque par dictionnaire
- ✔ Attaque par dictionnaire avec remplacement
- ✔ Etc…