جامعة شعيب الدكالي

Université Chouaib Doukkali

ÉTUDE DES SCHÉMAS DE FACTORİSATİON POUR CASSER LES CLÉS RSA À GRANDE ÉCHELLE

Presenter par :
AZLAG Nour El Hoda

Encadrer Par:
Pr. DAHMOUNI Abdellatif

Références

Boneh, D. (1999). "Twenty Years of Attacks on the RSA Cryptosystem". Notices of the AMS, 46(2), 203-213.

Plan

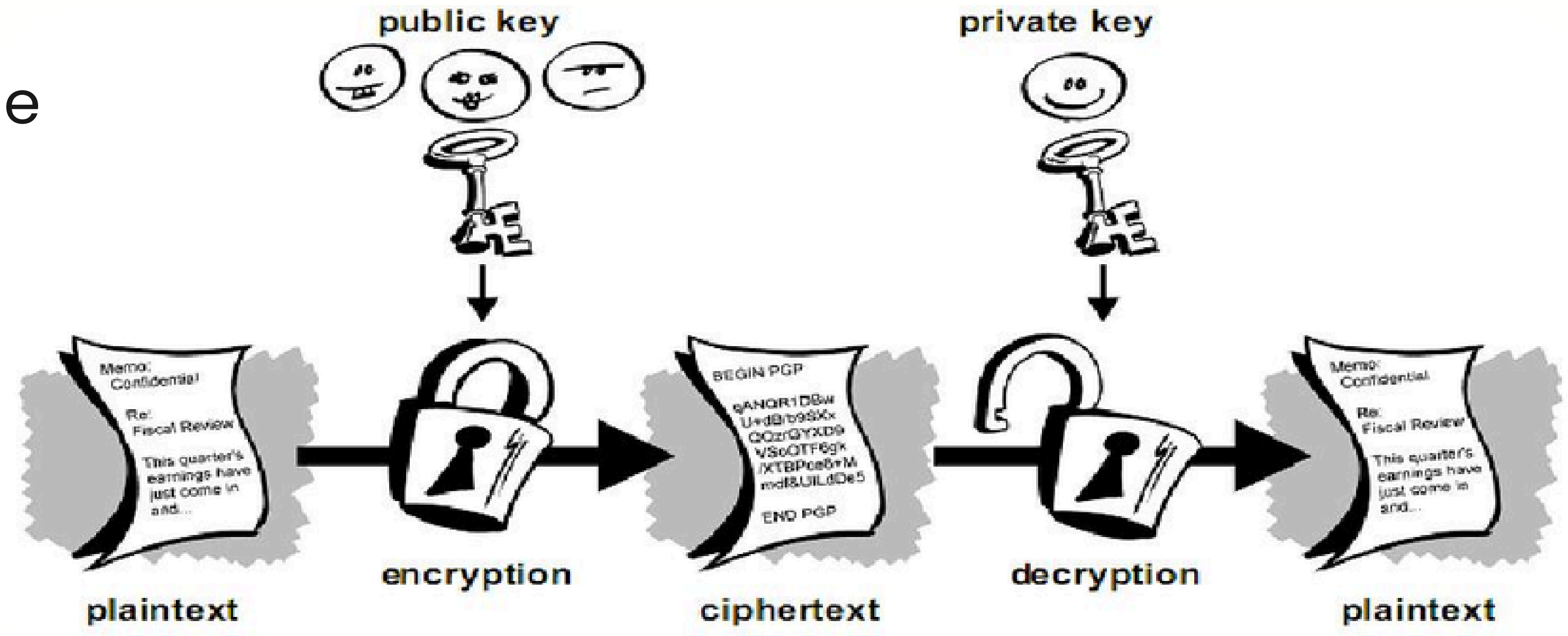
1
2
3
4
5
6
7
8
9

Introduction

- L' algorithme chiffrement RSA a été crée par Ronald Rivest, Adi Shamir et Leonard Adleman en 1977

- C'est un algorithme de cryptographie asymétrique

- Il est plus utilisé comme protocole dans le commerce électronique généralement pour échanger des données confidentielles sur Internet (https , TLS/SSL , …)



Rappels sur le fonctionnement de RSA

1
2
3
4
5
6
7
8
9

Les étapes de génération des clés:

- Choisir **p** et **q** premier entre eux
- Calculer **n= p*q**
- Calculer la fonction de Euler **φ(n)=(p-1)*(q-1)**
- Sélection **e** tel que **1<e<φ(n)** avec **PGCD(e, φ(n))=1.**
- Calculer **d** tel que **d*e≡ 1[φ(n)]**

Clé publique : (**n , e**)
Clé privée : **d**

Rappels sur le fonctionnement de RSA

1
2
3
4
5
6
7
8
9

Chiffrement :

Chiffrer le message **M** pour avoir le message **C**, on calcule :

$$C = M^{e} (\mathrm{mod}\ n)$$

Déchiffrement

Déchiffrer le message **C** pour avoir le message original **M**, on calcule :

$$M = C^{d} (\mathrm{mod}\ n)$$

1
2
3
4
5
6
7
8
9

Pourquoi la factorisation ?

- Le secret de RSA repose sur l’impossibilité de retrouver p et q à partir de n
- Si on factorise n → on calcule $\varphi(n)$ → on calcule d → RSA cassé
- État de l'art actuel :
  - RSA-512 : Cassé en 1999 (3,5 mois)
  - RSA-768 : Cassé en 2009 (2 ans)
  - RSA-1024 : Vulnérable (estimé 1-10 ans)
  - RSA-2048 : Sécurisé jusqu'en ~2030
  - RSA-4096 : Sécurisé au-delà de 2050
- À grande échelle, des méthodes sophistiquées permettent de casser RSA < 1024 bits

Les schémas de factorisation utilisés

- Méthode de factorisation directe
- Attaque du facteur commun

Méthode de factorisation directe

OBJECTIF :

Retrouver p et q à partir de n et φ(n)

MÉTHODE :

Transformer la factorisation en équation du 2nd degré

$$n = pq \text{ ET } \varphi(n) = (p-1)(q-1) \xrightarrow{\text{Chercher}} p = ? \text{ et } q = ?$$

1
2
3
4
5
6
7
8
9

Méthode de factorisation directe

Processus d'attaque étape par étape :

- Étape 1 : Développer $\varphi(n)$

$\varphi(n) = (p-1)(q-1)$

$\varphi(n) = pq - p - q + 1$

$\varphi(n) = n - p - q + 1$ [car $pq = n$]

- Étape 2 : Isoler $(p + q)$

$\varphi(n) = n + 1 - (p + q)$

$p + q = n + 1 - \varphi(n)$

- ÉTAPE 3 : Système d'équations

$\{ p + q = n + 1 - \varphi(n)$ (somme)

$\{ p \times q = n$ (produit)

Méthode de factorisation directe

1
2
3
4
5
6
7
8
9

- ÉTAPE 4 : Équation du second degré

Si **p** et **q** sont les racines d'une équation du second degré, alors cette équation s'écrit :

x^2 - (somme des racines)x + (produit des racines) = 0

Donc :

$x^2 - (p + q)x + pq = 0$

$x^2 - (n + 1 - \varphi(n))x + n = 0$

Méthode de factorisation directe

1
2
3
4
5
6
7
8
9

- ÉTAPE 5 : Calcul du discriminant

le discriminant est $\mathbf{\Delta = b^2 - 4ac}$

Dans notre cas : $x^2 - (n + 1 - \varphi(n))x + n = 0$

$\Delta = [-(n + 1 - \varphi(n))]^2 - 4(1)(n)$

$\Delta = (n + 1 - \varphi(n))^2 - 4n$

- ÉTAPE 6 : Solutions de l'équation

Les solutions d'une équation du second degré sont :

$x = (-b \pm \sqrt{\Delta}) / 2a$

Dans notre cas : $x = (n + 1 - \varphi(n) \pm \sqrt{\Delta}) / 2$

Les deux solutions sont p et q :

$p = (n + 1 - \varphi(n) + \sqrt{\Delta}) / 2$ $q = (n + 1 - \varphi(n) - \sqrt{\Delta}) / 2$

Méthode de factorisation directe

Exemple:

Données initiales :

$n = 3233$ (nombre public)

$\varphi(n) = 3120$ (supposé connu par l'attaquant)

1
2
3
4
5
6
7
8
9

Méthode de factorisation directe

Processus d'attaque étape par étape :

- Étape 1 : Calculer p + q

$$p + q = n + 1 - \varphi(n)$$

$$p + q = 3233 + 1 - 3120 = 114$$

- Étape 2 : Calculer le discriminant

$$\Delta = (p + q)^2 - 4n$$

$$\Delta = 114^2 - 4 \times 3233$$

$$\Delta = 12996 - 12932 = 64$$

1
2
3
4
5
6
7
8
9

Méthode de factorisation directe

Processus d'attaque étape par étape :

- Étape 3 : Calculer $\sqrt{\Delta}$

  $\sqrt{\Delta} = \sqrt{64} = 8$

- Étape 4 : Trouver p et q

  $p = (114 + 8) \div 2 = 122 \div 2 = 61$

  $q = (114 - 8) \div 2 = 106 \div 2 = 53$

Méthode de factorisation directe

1
2
3
4
5
6
7
8
9

Vérification :

- $n = p \times q = 61 \times 53 = 3233$ ✓
- $\varphi(n) = (p-1) \times (q-1) = 60 \times 52 = 3120$ ✓

Attaque du facteur commun

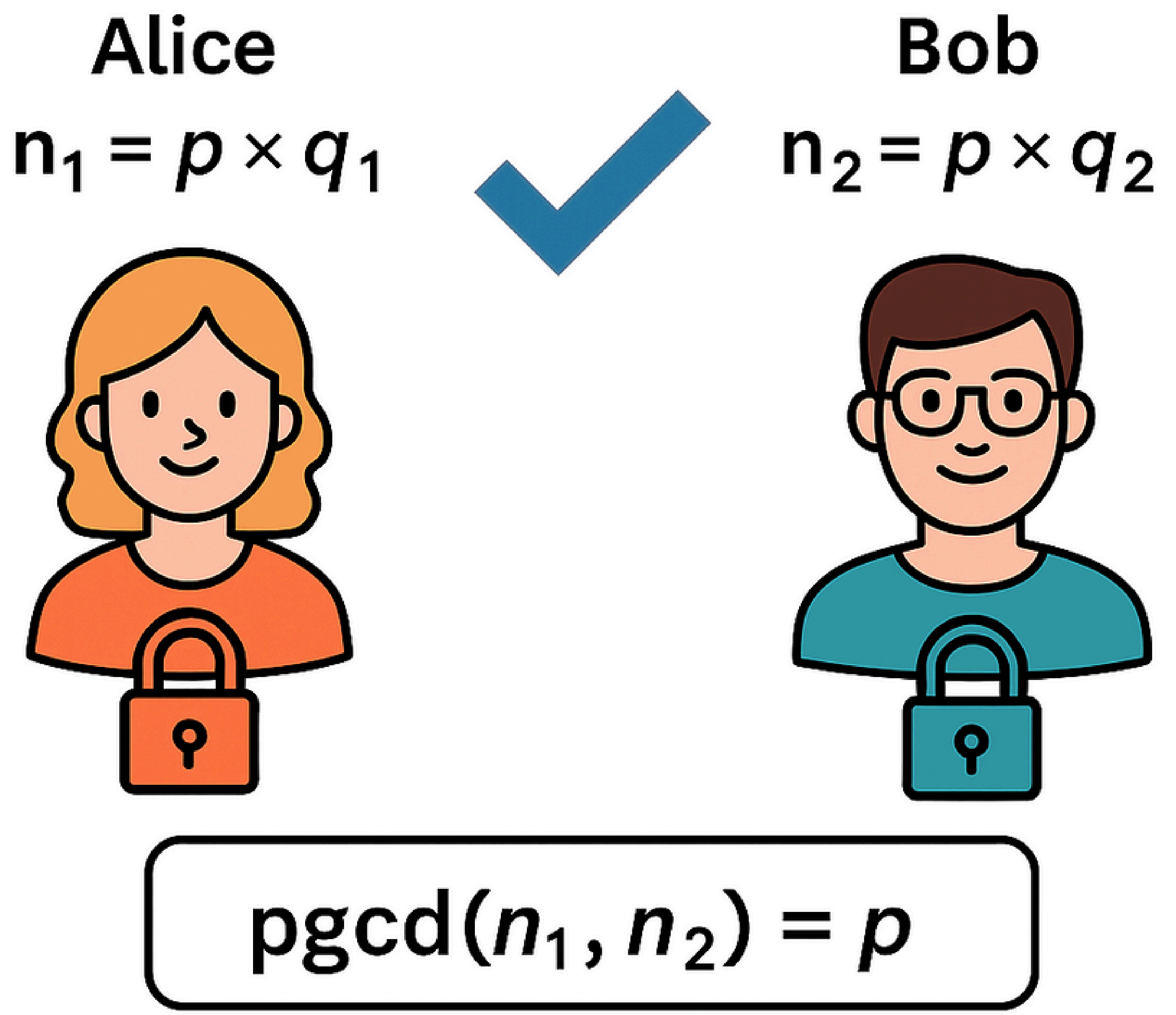
"Si deux secrets partagent un élément commun,

ce n'est plus un secret !"

Attaque du facteur commun

Parfois, deux clés RSA différentes partagent accidentellement un facteur premier

Problème : ils ont utilisé le **même p** !



Attaque du facteur commun

- Calculer **PGCD(n_1, n_2)**

  => Si pgcd > 1 → c'est le facteur commun p !

- Calculer les autres facteurs :

  $$q_1 = n_1 \div p \text{ et } q_2 = n_2 \div p$$

- Les deux clés RSA sont cassées !

Attaque du facteur commun

1
2
3
4
5
6
7
8
9

Exemple

Données initiales :

- $n_1 = 3233$
- $n_2 = 4087$

Attaque du facteur commun

Processus d'attaque étape par étape :

- Calcul du PGCD (Algorithme d'Euclide)

$$4087 = 1 \times 3233 + 854$$

$$3233 = 3 \times 854 + 671$$

$$854 = 1 \times 671 + 183$$

$$671 = 3 \times 183 + 122$$

$$183 = 1 \times 122 + 61$$

$$122 = 2 \times 61 + 0$$

-->PGCD(3233, 4087) = 61

Attaque du facteur commun

Processus d'attaque étape par étape :

- FACTEURS RÉVÉLÉS :
  - Facteur commun : $p = 61$
  - Alice : $q_1 = 3233 \div 61 = 53 \rightarrow n_1 = 61 \times 53$
  - Bob : $q_2 = 4087 \div 61 = 67 \rightarrow n_2 = 61 \times 67$

Attaque du facteur commun

1
2
3
4
5
6
7
8
9

- **Cas réel impressionnant** :

En 2012, des chercheurs ont scanné Internet et trouvé 12 720 clés RSA publiques vulnérables à cette attaque ! Ils ont pu factoriser 0,2% de toutes les clés RSA disponibles publiquement.

1
2
3
4
5
6
7
8
9

Demo

Conlusion

- RSA reste sûr, mais seulement avec des clés suffisamment longues (≥ 2048 bits)
- Les erreurs humaines ou techniques (ex. facteur commun) rendent RSA vulnérable

“Comprendre comment casser RSA, c’est aussi mieux savoir le protéger.”

1

2

3

4

5

6

7

8

9

Merci