Cryptanalyse sur un cluster de PlayStation 3

Maxime Augier, Nathalie Casati, Dag Arne Osvik
LACAL

16 avril 2008

Laboratory for Cryptologic Algorithms

Etude des méthodes mathématiques permettant de protéger certaines informations voyageant sur internet (ou d'autres réseaux ouverts).

Laboratory for Cryptologic Algorithms

Etude des méthodes mathématiques permettant de protéger certaines informations voyageant sur internet (ou d'autres réseaux ouverts).

Deux sujets principaux :

- Comment rendre ces moyens de protection encore plus « invisibles » à l'utilisateur tout en les améliorant

Laboratory for Cryptologic Algorithms

Etude des méthodes mathématiques permettant de protéger certaines informations voyageant sur internet (ou d'autres réseaux ouverts).

Deux sujets principaux :

- Comment rendre ces moyens de protection encore plus « invisibles » à l'utilisateur tout en les améliorant
- Evaluation du niveau de sécurité obtenu lors de l'utilisation de ces algorithmes de protection en développant des « estimations » de la puissance de calcul nécessaire pour les attaquer avec succès

Définition

La **cryptographie** (étymologiquement « écriture secrète ») est une science visant à cacher l'information sémantique d'un texte de manière à rendre son contenu inintelligible par des personnes non autorisées à l'accéder.

Définition

La **cryptographie** (étymologiquement « écriture secrète ») est une science visant à cacher l'information sémantique d'un texte de manière à rendre son contenu inintelligible par des personnes non autorisées à l'accéder.

Définition

Le **chiffrement** est l'action de transformer un texte en message crypté (cryptogramme) à l'aide d'un algorithme utilisant une clé secrète.

Définition

La **cryptanalyse** est la science étudiant les moyens de décrypter ces cryptogrammes sans connaître la clé, de manière à tester la sécurité de l'algorithme utilisé pour le chiffrement.

Définition

La **cryptanalyse** est la science étudiant les moyens de décrypter ces cryptogrammes sans connaître la clé, de manière à tester la sécurité de l'algorithme utilisé pour le chiffrement.

Cryptologie = Cryptographie + Cryptanalyse

Durant cette démonstration, nous allons décrypter un cryptogramme chiffré avec l'un de ces algorithmes à l'aide d'une PlayStation 3 (sans connaître la clé)

Un algorithme de chiffrement : DES

- Sert à maintenir la confidentialité d'une information au moment où elle est transmise sur un réseau non sécurisé (comme internet)

Un algorithme de chiffrement : DES

- Sert à maintenir la confidentialité d'une information au moment où elle est transmise sur un réseau non sécurisé (comme internet)
- Introduit au milieu des années 70, collaboration entre IBM et la NSA

Un algorithme de chiffrement : DES

- Sert à maintenir la confidentialité d'une information au moment où elle est transmise sur un réseau non sécurisé (comme internet)
- Introduit au milieu des années 70, collaboration entre IBM et la NSA
- La longueur de la clé (56 bits) étant trop petite, il est aujourd'hui possible de les essayer toutes

Un algorithme de chiffrement : DES

- Sert à maintenir la confidentialité d'une information au moment où elle est transmise sur un réseau non sécurisé (comme internet)
- Introduit au milieu des années 70, collaboration entre IBM et la NSA
- La longueur de la clé (56 bits) étant trop petite, il est aujourd'hui possible de les essayer toutes
- A ce jour, la force brute est toujours le seul moyen d'attaquer DES, mais il existe des attaques théoriques plus rapides

Un algorithme de chiffrement : DES

- Sert à maintenir la confidentialité d'une information au moment où elle est transmise sur un réseau non sécurisé (comme internet)
- Introduit au milieu des années 70, collaboration entre IBM et la NSA
- La longueur de la clé (56 bits) étant trop petite, il est aujourd'hui possible de les essayer toutes
- A ce jour, la force brute est toujours le seul moyen d'attaquer DES, mais il existe des attaques théoriques plus rapides
- DES est toujours beaucoup utilisé (ça coûte plus cher d'améliorer un système que de risquer une attaque)

Au milieu des années 90 :

- on estime que DES a toujours entre une demie et 3 quarts du marché des produits nécessitant un chiffrement
- les produits utilisant DES aux Etats-Unis rapportent entre $75 et $125 mio par année
- DES a été trouvé dans ≈un millier de produits domestiques de chiffrement

Au milieu des années 90 :

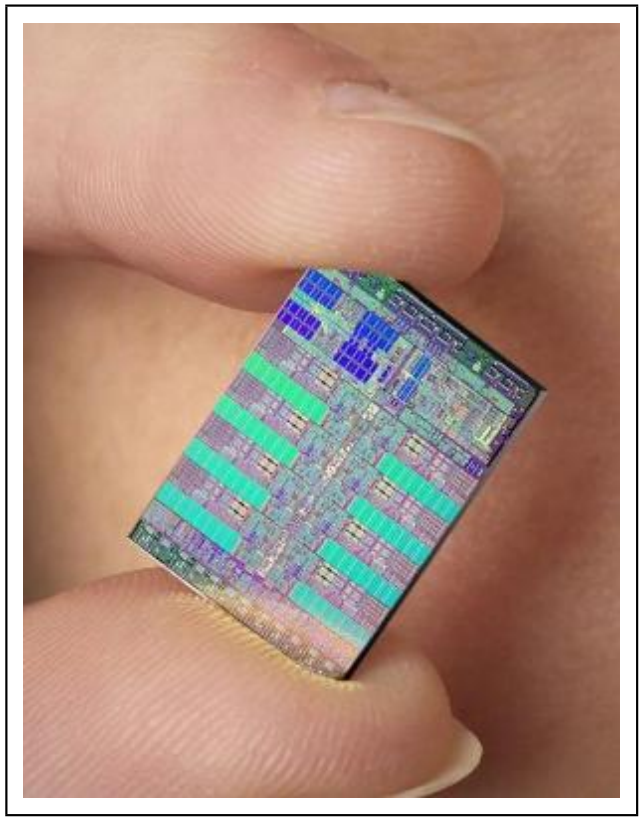
- on estime que DES a toujours entre une demie et 3 quarts du marché des produits nécessitant un chiffrement
- les produits utilisant DES aux Etats-Unis rapportent entre \$75 et \$125 mio par année
- DES a été trouvé dans ≈un millier de produits domestiques de chiffrement

Exemples (actuels) :

- Transferts entre les bancomats et les banques
- Trafic interne des banques
- Communications « sécurisées » sur Amazon
- etc.

Message	”SOLEIL”
Clé	0x 23 45 67 89 AB CD EF 01
Cryptogramme	|4«v×Rº´

Le processeur Cell



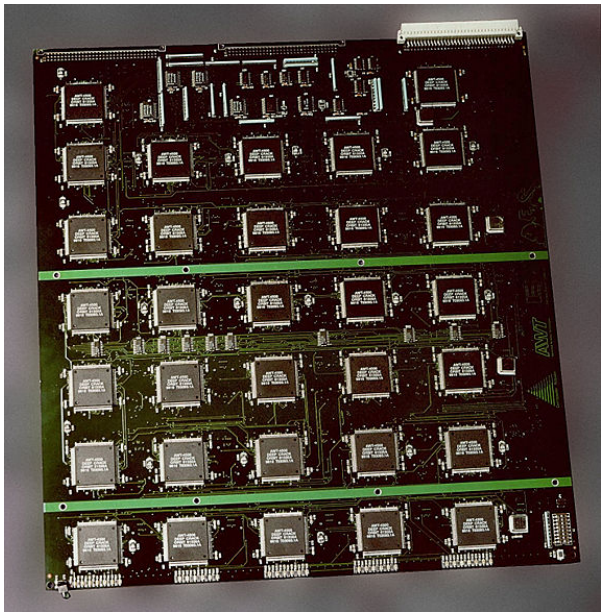
- 1 PowerPC Processing Unit
- 8 Synergistic Processor Units
- Fréquence 3.2GHz

Le processeur Cell

- Fruit d'une alliance entre Sony, Toshiba et IBM
- Sorti en fin 2005
- 4 ans de développement
- budget de $400 mio

Un PC ou une PlayStation 3 ?

	Machine Intel	PlayStation 3
Prix	$500	$500
Blocs/sec/unité de calcul	16M	64M
Unités de calcul	4	6



	DES Cracker	PS3 cluster
Prix	$250'000	$120'000
Temps	9 jours	6 jours
Clés/sec	88.8 mia	142.5 mia
Unités de calcul	37050	1320
Année	1999	2009

Explications

On va casser une clé de 36 bits ≈20 minutes

1. Séparez-vous en 2 groupes

Explications

On va casser une clé de 36 bits ≈20 minutes

1. Séparez-vous en 2 groupes
2. Ecrivez un message « confidentiel » de type e-mail à l'autre groupe à l'aide de l'éditeur de texte

Explications

On va casser une clé de 36 bits ≈20 minutes

1. Séparez-vous en 2 groupes
2. Ecrivez un message « confidentiel » de type e-mail à l'autre groupe à l'aide de l'éditeur de texte
3. Sauvez le message sur le bureau en encodage ISO-8859-1

Explications

On va casser une clé de 36 bits ≈20 minutes

1. Séparez-vous en 2 groupes
2. Ecrivez un message « confidentiel » de type e-mail à l'autre groupe à l'aide de l'éditeur de texte
3. Sauvez le message sur le bureau en encodage ISO-8859-1
4. Glissez-le sur l'icône de l'application « Chiffrer » et suivez les instructions

Explications

On va casser une clé de 36 bits ≈20 minutes

1. Séparez-vous en 2 groupes
2. Ecrivez un message « confidentiel » de type e-mail à l'autre groupe à l'aide de l'éditeur de texte
3. Sauvez le message sur le bureau en encodage ISO-8859-1
4. Glissez-le sur l'icône de l'application « Chiffrer » et suivez les instructions
5. Pour vérifier que vous pouvez le décrypter, glissez le fichier .des généré sur l'application « Décrypter »

Explications

On va casser une clé de 36 bits ≈20 minutes

1. Séparez-vous en 2 groupes
2. Ecrivez un message « confidentiel » de type e-mail à l'autre groupe à l'aide de l'éditeur de texte
3. Sauvez le message sur le bureau en encodage ISO-8859-1
4. Glissez-le sur l'icône de l'application « Chiffrer » et suivez les instructions
5. Pour vérifier que vous pouvez le décrypter, glissez le fichier .des généré sur l'application « Décrypter »
6. Copier le message sur la clé USB et la remettre à Dag Arne

Explications

On va casser une clé de 36 bits ≈20 minutes

1. Séparez-vous en 2 groupes
2. Ecrivez un message « confidentiel » de type e-mail à l'autre groupe à l'aide de l'éditeur de texte
3. Sauvez le message sur le bureau en encodage ISO-8859-1
4. Glissez-le sur l'icône de l'application « Chiffrer » et suivez les instructions
5. Pour vérifier que vous pouvez le décrypter, glissez le fichier .des généré sur l'application « Décrypter »
6. Copier le message sur la clé USB et la remettre à Dag Arne

Dag Arne symbolise internet, où votre message pourra être intercepté avant d'atteindre l'autre groupe

Explications

A l'aide de deux PlayStation 3, nous allons tenter de décrypter les messages confidentiels que vous vouliez transmettre à vos collègues

Départ pour la visite !

Questions ?