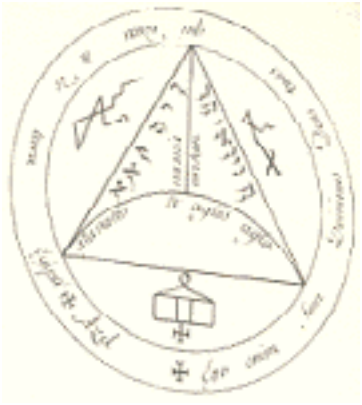

Cours individuel de cryptanalyse

1 Introduction

Depuis que j'ai écrit ***Cryptographie appliquée***, on m'a demandé de recommander un livre sur la cryptanalyse. Ma malheureuse réponse est que bien qu'il existe plusieurs bon livres sur la cryptographie, il n'y a pas de livres, bon ou mauvais, sur la cryptanalyse. C'est un vide que je ne vois pas comblé avant un long moment ; la cryptanalyse est un domaine qui évolue si rapidement qu'un livre sur ces techniques serait obsolète avant même son impression. Et même si le livre parvenait à rester actuel, il ne ferait que peu pour enseigner la cryptanalyse.

Le seul moyen d'apprendre la cryptanalyse est au travers de la pratique. Un étudiant doit simplement briser algorithme après algorithme, inventer de nouvelles techniques et modifier celles qui existent. Lire les résultats des autres cryptanalyses aidera, mais il n'y a aucun substitut à l'expérience.

Cette réponse en amène une autre : où peut-t'on obtenir de l'entraînement? Internet est une source sans fin de conceptions médiocres d'algorithmes, et même certains traînent dans la littérature académique, mais l'étudiant apprenti en cryptanalyse n'a aucun moyen de savoir quels algorithmes valent une étude, et quels sont ceux qui sont au-delà de ses capacités. Essayer de briser des algorithmes qui ont déjà été brisés (sans regarder comment ils ont été brisés) est la seule réponse.

Maintenant la question devient: quels chiffrements faut-t'il essayer de briser et dans quel ordre? Ce document est ma tentative de réponse, et dans cette réponse, j'espère faciliter l'étude de la cryptanalyse.

Ceci forme un apprentissage individuel de la cryptanalyse des chiffrements par bloc. Avec, un étudiant peut suivre un chemin ordonné au travers de la littérature académique et ressortir de l'autre côté en étant capable de briser de nouveaux algorithmes et de publier de nouveaux résultats cryptanalytiques.

Ce que j'ai fait, c'est lister les algorithmes publiés et les cryptanalyses, dans un ordre cohérent: par type de cryptanalyse et difficulté. La tâche de l'étudiant est de lire les documents qui décrivent les algorithmes, puis tenter de reproduire les résultats cryptanalytiques (et il est beaucoup plus difficile d'apprendre la cryptanalyse à partir des documents académiques que de livres distillés, mais tôt ou tard l'étudiant devra apprendre à lire les documents académiques, et le plus tôt sera le mieux). Les résultats, dans les documents publiés, serviront de "clefs de réponse".

La réponse clef n'est jamais définitive ; il est très probable qu'il existe d'autres, et de meilleures, attaques que celles qui ont été publiées. Certains documents cryptanalytiques contiennent des erreurs. Les étudiants qui vont entamer ce cours devraient finir par être capables de publier eux-mêmes des résultats publiables.

Même le meilleur étudiant ne sera pas capable de trouver tous les moyens de briser les algorithmes sans consulter les documents de cryptanalyse. Beaucoup de ces résultats ont été découverts par les plus grands esprits de la cryptanalyse. Je pense qu'un étudiant doit consacrer au minimum une semaine à chaque algorithme avant de commencer à consulter le document cryptogamique, et après avoir rapidement parcouru le résultat ; ou avoir juste lu le résumé, l'introduction et la conclusion il devra à nouveau chercher à briser l'algorithme pendant encore trois jours.

Si l'étudiant ne parvient toujours pas à briser le chiffrement, il sera temps de lire et d'étudier la cryptanalyse publiée. Si l'étudiant ne parvient pas à briser le moindre chiffrement en particulier ceux qui sont faciles c'est une bonne indication qu'il devrait trouver une autre occupation.

Les leçons sont ordonnées, mais cet ordre reste relativement souple. Les premières leçons sont faciles, mais je mélange un peu les choses par la suite. Les étudiants sont libres de passer les leçons qui leur semblent difficiles, puis d'y revenir plus tard, et même d'en passer certaines complètement (il y en a beaucoup). Mon intention n'est pas d'attendre de chaque étudiant qu'il complète la leçon complètement avant de passer à la suivante. Un étudiant intelligent sera probablement capable de travailler sur plusieurs leçons en même temps.

Bonne chance.

2 Que signifie "briser" un chiffrement?

Briser un chiffrement ne signifie pas nécessairement trouver un moyen pratique pour une personne à l'écoute de récupérer le texte en clair en utilisant seulement le texte chiffré. Dans la cryptographie académique, les règles sont beaucoup plus souples. Briser un chiffrement revient à trouver une faiblesse dans le chiffrement qui peut être exploitée avec une complexité inférieure à une attaque de force brute. Peu importe que l'attaque par force brute requiert 2^{128} chiffrements ; une attaque demandant 2^{110} chiffrements sera considérée comme un succès. Briser un chiffrement pourrait aussi demander un nombre non-réaliste de textes en clair choisis, 2^{56} blocs, ou bien des quantités irréalistes de stockage : 2^{80}. Simplement dit, briser un algorithme peut être une "faiblesse certifiée" : une preuve que le chiffrement ne fonctionne pas comme prévu.

Une cryptanalyse réussie peut signifier la révélation d'un brisement d'une forme réduite du chiffrement, un DES de 8 rondes contre les 16 rondes formant un DES complet, par exemple ou une variante simplifiée du chiffrement. La plupart des cryptanalyses commencent par une cryptanalyse d'une variante aux nombres de rondes réduites, et sont éventuellement (parfois des années plus tard) étendues au chiffrement complet.

3 Pourquoi les chiffrements par blocs?

La recherche académique sur les chiffrements par blocs ont progressé sur une voie différente de la recherche des chiffrements de flux. Les documents sur les chiffrements par blocs ont traditionnellement été des conceptions concrètes (avec des paramètres et des noms spécifiques) ou des conceptions brisées. Les documents sur les chiffrements de flux sont plus souvent des conceptions générales ou des techniques d'analyse, avec des applications et des exemples généraux.

Bien que la cryptanalyse des chiffrements de flux soit aussi importante que les chiffrements par blocs, et encore plus dans le cercle militaire, il est beaucoup plus difficile de former un cours combinant les deux à partir des documents académiques existants. Un bon document de survol des chiffrements de flux est disponible en-ligne à l'adresse :
http://www.rsa.com/rsalabs/pubs/html/notes.html

4 Pré-requis

Il sera pratiquement impossible de comprendre certains résultats cryptanalytiques sans une bonne compréhension de concepts simples des probabilités et statistiques. Le ***Handbook of Applied Cryptography*** dispose d'une introduction rapide sur une grande partie de la théorie des probabilités ; toutefois, les étudiants qui apprennent ces domaines pour la première fois trouveront une introduction plus douce au sujet dans un livre consacré aux probabilités et statistiques.

D'autres sujets des mathématiques discrètes et de la science informatique seront aussi utiles, bien qu'ils ne soient pas strictement indispensables. Un étudiant devrait apprendre, ou être prêt à apprendre, l'algèbre linéaire, la théorie des groupes, la théorie de la complexité, le combinatoire et la théorie des graphes. Ces domaines devraient être étudiés profitablement avec la cryptanalyse.

Il est impossible de comprendre réellement une attaque cryptanalytique sans l'implémenter. ***Implémenter*** une attaque décrite dans un document peut être très instructif ; implémenter une nouvelle attaque de votre cru révèle souvent des subtilités que l'analyse théorique ne pourra analyser. Pour cette raison, la programmation mathématique dans un langage tel que le C est une compétence requise.

4.1 Fond historique

La cryptanalyse des algorithmes de chiffrement avant l'avènement des ordinateurs n'est pas réellement applicable à la cryptanalyse des algorithmes modernes, mais elle forme une lecture intéressante et offre un bon exemple de l'état d'esprit requis pour réaliser de la cryptanalyse. Je ne considère pas cela comme un requis indispensable, mais un étudiant appliqué devrait considérer la lecture d'Helen Fourche Gaines, ***Cryptanalysis: A Study of Ciphers and their Solution*** (Dover Publications, 1939). Sont aussi intéressants: les volumes écrits par William F. Friedman et réimprimés par Agean Park Press:

- ***Elements of Cryptanalysis***
- ***Military Cryptanalysis,*** parties I, II, III et IV
- ***The Riverbank Publications,*** parties I, II et III
- ***Military Cryptanalytics,*** partie I, vol.1 et 2 et partie II, vol.1 et 2.

Aegan Press se trouve à l'adresse http://www.ageanpress.com/books/

Une lecture attentive de David Kahn, ***The Codebreakers*** (The Macmillan Company, 1967) est indispensable pour une compréhension de l'histoire de la cryptographie. Je le recommande fortement.

5 Obtenir les matériaux de cours

Les documents utilisés dans ce cours proviennent des travaux de plusieurs conférences différentes. J'ai tenté d'éviter les publications obscures, mais invariablement vous en trouverez. Ceci signifie que beaucoup de bons chiffrements ne sont pas listés ci-dessus : CAST est le premier exemple. S'il vous plaît ne

considérez pas l'absence d'un chiffrement de la liste comme une indication de force ou de faiblesse, c'est tout simplement une question de disponibilité.

Pratiquement tous les documents proviennent des travaux des conférences Springer-Verlag, tous publiés dans les séries ***Lecture Notes in Computer Science (LNCS).*** La plupart des librairies universitaires souscrivent aux séries LNCS complètes. Au minimum, un étudiant devrait disposer du cédérom contenant les travaux de tous les Crypto et Eurocrypt (disponible chez Springer-Verlag), ainsi que les travaux provenant des séries ***Fast Software Encryption (FSE).*** Il y a beaucoup de documents dans ces travaux dont la lecture est bénéfique, bien qu'ils ne soient pas listés ici.

Je maintiens une page à http://www.counterpane.com avec des liens vers les documents disponibles sur la toile. Au-travers du cédérom, des travaux FSE et de mes ressources Internet, il est possible de réaliser pratiquement tout ce qui est dans ce cours.

6 Le cours

6.1 Historique

Lisez au moins les livres :

- B. Schneier, ***Cryptographie appliquée, seconde édition*** (John Wiley & Sons, 1996).
- D.R. Stinson, ***Cryptography: Theory and Practice*** (CRC Press, 1995).
- A.J. Menezes, P.C. van Oorschot et S.A. Vanstone, ***Handbook of Applied Cryptography*** (CRC Press, 1997).

Concentrez-vous sur les chapitres consacrés aux chiffrements par blocs, bien que je vous recommande fortement la lecture complète de chaque livre.

6.2 Cryptanalyse de base

Essayez de cryptanalyser les algorithmes suivants, simplifiés :

- RC5 à 8 rondes sans aucune rotation.
- RC5 à 8 rondes avec un nombre de rotations égal au nombre de rondes.
- DES à 12 rondes sans aucune Table-S.
- Skipjack à 8 rondes en règle B (une description de Skipjack peut être trouvée sur Internet)
- DES à 4 rondes.
- Un chiffrement générique qui est "fermé" (i.e. chiffrer avec la clef A puis la clef B revient au même qu'un chiffrement avec la clef C, pour toutes les clefs).
- DES à 6 rondes.
- Skipjack à 4 rondes en règle A suivi par 4 rondes de Skipjack en règle B.

Tous ces algorithmes sont décrits dans le livre de B. Schneier, ***Cryptographie appliquée, seconde édition*** (John Wiley & Sons, 1996) et A.J. Menezes, P.C. van Oorschot et S.A. Vanstone, ***Handbook of Applied Cryptography*** (CRC Press, 1997).

6.3 Cryptanalyse de FEAL

Il semble que toute attaque de cryptanalyse moderne fonctionne contre FEAL. Lisez d'abord le premier algorithme:

A. Shimizu et S. Miyaguchi, "Fast Data Enciphering Algorithm FEAL"
Advances in Cryptology EUROCRYPT '87 Proceedings,
Springer-Verlag, 1988, pp. 267-278

Puis tentez de le briser. Certaines attaques peuvent être trouvées dans:

B. Den Boer, "Cryptanalysis of F.E.A.L."
Advances in Cryptology ; EUROCRYPT '88 Proceedings,
Springer-Verlag, 1988, pp. 275-280

H. Gilbert et P. Chasse, "A Statistical Attack on the FEAL-8 Cryptosystem"
Advances in Cryptology CRYPTO '90 Proceedings,
Springer-Verlag, 1991, pp. 22-33

A. Tardy-Cordfir et H. Gilbert, "A Known Plaintext Attack of FEAL-4 and FEAL-6"
Advances in Cryptology CRYPTO '91 Proceedings,
Springer-Verlag, 1992, pp. 172-182

Vous pouvez aussi réinventer les cryptanalyses différentielles et linéaires si vous travaillez assez dur.

6.4 Cryptanalyse différentielle

Lisez les chapitres 1 à 5 de:

E. Biham et A. Shamir,
Differential Cryptanalysis of the Data Encryption Standard
(Springer-Verlag, 1993).

Si vous ne trouvez pas le livre, lisez:

E. Biham et A. Shamir, "Differential Cryptanalysis of the Full 16-Round DES",
Advances in Cryptology CRYPTO '91 Proceedings, Springer-Verlag, 1992,
pp. 487-496.

6.5 Cryptanalyse différentielle de FEAL

Attaquez FEAL en utilisant la cryptanalyse différentielle. Une solution, qui est le premier document à parler des attaques différentielles, est de:

S. Murphy, "The Cryptanalysis of FEAL-4 with 20 Chosen Plaintexts",
Journal of Cryptology, v.2, n.3, 1990, pp. 145-154.

Consultez aussi le chapitre 6 de:

E. Biham et A. Shamir,
Differential Cryptanalysis of the Data Encryption Standard
(Springer-Verlag, 1993).

6.6 Cryptanalyse différentielle de LOKI-89

La première version de LOKI est désormais appelée LOKI-89. Lisez:

L. Brown, J. Pieprzyk et J. Seberry,
"LOKI: A Cryptographic Primitive for Authentification and Secrecy Applications",
Advances in Cryptology AUSCRYPT '90 Proceedings,
Springer-Verlag, 1990, pp. 229-236.

Trouvez une attaque différentielle; une solution se trouve dans:

L.R. Knudsen, "Cryptanalysis of LOKI",
Advances in Cryptology ASIACRYPT '91, Springer-Verlag, 1993, pp. 22-35.

Le livre de Biham et Shamir aborde aussi cette cryptanalyse.

6.7 Cryptanalyse différentielle de MacGuffin

Lisez:

M. Blaze et B. Schneier, "The MacGuffin Block Cipher Algorithm",
Fast Software Encryption, Second International Workshop Proceedings,
Springer-Verlag, 1995, pp. 97-110.

Essayez de briser le chiffrement. Une attaque différentielle se trouve dans:

V. Rijmen et B. Preneel, "Cryptanalysis of MacGuffin",
Fast Software Encryption, Second International Workshop Proceedings,
Springer-Verlag, 1995, pp. 353-358.

Il y a beaucoup plus d'attaques, dont certaines n'ont jamais été publiées. Il est bénéfique de consacrer du temps à cet algorithme, même s'il faut pour cela y revenir plus tard au cours de votre apprentissage. A mesure que vous apprendrez de nouvelles techniques, vous découvrirez de nouvelles attaques.

6.8 Cryptanalyse différentielle de Khafre

Lisez la description de Khafre dans:

R.C. Merkle, "Fast Software Encryption Functions",
Advances in Cryptology CRYPTO '91 Proceedings,
Springer-Verlag, 1992, pp. 156-171

Consultez aussi le livre de Biham et Shamir.

6.9 Cryptanalyse différentielle de PES

Le précurseur de l'IDEA fut le PES; consultez:

X. Lai et J. Massey, "A Proposal for a New Block Encryption Standard"
Advances in Cryptology EUROCRYPT '90 Proceedings,
Springer-Verlag, 1991, pp. 389-404

Essayez de le briser en utilisant la cryptanalyse différentielle. Les résultats (et une reconception) sont disponibles dans:

X. Lai, J. Massey et S. Murphy, "Markov Ciphers and Differential Cryptanalysis",
Advances in Cryptology EUROCRYPT '91 Proceedings,
Springer-Verlag, 1991, pp. 17-38.

6.10 Cryptanalyse linéaire

Lisez:

M. Matsui, "Linear Cryptanalysis Method for DES Cipher",
Advances in Cryptology EUROCRYPT '93 Proceedings,
Springer-Verlag, 1994, pp. 386-397

Essayez d'améliorer les résultats. Une solution se trouve dans:

M. Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard",
Advances in Cryptology CRYPTO '94 Proceedings,
Springer-Verlag, 1994, pp. 1-11

6.11 Cryptanalyse linéaire de FEAL

Essayez de casser FEAL en utilisant les techniques de cryptanalyse linéaire. Des solutions se trouvent dans:

M. Matsui et A. Yamagishi,
"A New Method for Known Plaintext Attack of FEAL Cipher",
Advances in Cryptology EUROCRYPT '92 Proceedings,
Springer-Verlag, 1993, pp. 81-91

et:

K. Ohta et K. Aoki, "Linear Cryptanalysis of the Fast Data Encipherment Algorithm",
Advances in Cryptology CRYPTO '94 Proceedings,
Springer-Verlag, 1994, pp. 12-16

Consultez aussi:

S. Moriai, K. Aoki et K. Ohta,
"Improving the Search Algorithm for the Best Linear Expression",
Advances in Cryptology CRYPTO '95 Proceedings,
Springer-Verlag, 1995, pp. 157-170

6.12 Caractéristiques différentielles conditionnelles

Les caractéristiques conditionnelles ont été introduites par:

I. Ben-Aroya et E. Biham, "Differential Cryptanalysis of Lucifer",
Advances in Cryptology CRYPTO '93 Proceedings,
Springer-Verlag, 1994, pp. 187-199

Lisez les sections 1-3, sur Lucifer et les caractéristiques conditionnelles. Essayez ensuite de trouver une attaque avant de lire la section 4. Lisez le début de la section 5, sur le RDES. Essayez de trouver l'attaque avant de lire la suite du document.

6.13 Cryptanalyse par rotation des clefs-liées

Lisez les résultats contre LOKI-89 et LOKI-91 dans:

E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys",
Journal of Cryptology, v.7, n.4, 1994, pp. 229-246.

Si vous ne trouvez pas le journal, lisez la copie préliminaire (***Advances in Cryptology EUROCRYPT '93,*** Springer-Verlag, 1994, pp. 398-409.

Attaquez la variante du DES décrite dans la section 5 (la section 6 dans la version EuroCrypt).

6.14 Cryptanalyse différentielle-linéaire

Lisez:

S. Langford et M. Hellman, "Differential-Linear Cryptanalysis",
Advances in Cryptology CRYPTO '94 Proceedings,
Springer-Verlag, 1994, pp. 17-26

Essayez d'appliquer ces techniques à FEAL. La réponse se trouve dans:

K. Aoki et K. Ohta, "Differential-Linear Cryptanalysis of FEAL-8",
IEICE Transactions: Fundamentals of Electronics, Communications, and Computer Sciences (Japan), v. E79-A, n.1, 1996, pp. 20-27.

Bonne chance pour trouver le journal ci-dessus: c'est un journal japonais.

6.15 Relations entre les cryptanalyses différentielles et linéaires

Lisez:

E. Biham, "On Matsui's Linear Cryptanalysis",
Advances in Cryptology EUROCRYPT '94 Proceedings,
Springer-Verlag, 1995, pp. 398-412

et dans:

F. Chabaud et S. Vaudenay,
"Links Between Differential and Linear Cryptanalysis",
Advances in Cryptology EUROCRYPT '94 Proceedings,
Springer-Verlag, 1995, pp. 356-365

6.16 Cryptanalyse différentielle de haut-ordre

Si vous pouvez le trouver, lisez:

X. Lai, "Higher Order Derivatives and Differential Cryptanalysis",
Communications and Cryptography, Kluwer Academic Publishers, 1994,
pp. 227-233

Lisez la section 4 de:

L.R. Knudsen, "Truncated and Higher Order Differentials",
Fast Software Encryption, 2nd International Workshop Proceedings,
Springer-Verlag, 1995, pp. 196-211

6.17 Cryptanalyse par différentielles de haut-ordre du chiffrement-KN

Lisez:

K. Nyberg et L.R. Knudsen, "Provable Securiy Against Differential Cryptanalysis",
Journal of Cryptology, v.8, n.1, 1995, pp. 27-37

Le chiffrement dans la section 5 est appelé chiffrement-KN; essayez de le briser en utilisant les différentielles de haut-ordre. Kiefer est aussi décrit dans:

K. Kiefer, "A New Design Concept for Building Secure Block Ciphers",
Proceedings of Pragocrypt '96, CTU Publishing House, 1996, pp. 30-41

Une bonne solution :

T. Shimoyama, S. Moriai et T. Kaneko,
"Improving the Higher Order Differential Attack and Cryptanalysis of the KN Cipher",
Information Security, First International Workshop ISW '97 Proceedings,
Springer-Verlag, 1998, pp. 32-42

6.18 Estimations linéaires multiples

Lisez:

B. Kaliski Jr et M. Robshaw, "Linear Cryptanalysis Using Multiple Approximations",
Advances in Cryptology CRYPTO '94 Proceedings,
Springer-Verlag, 1994, pp. 26-39

Essayez de briser FEAL en utilisant ces techniques. Une solution est:

B. Kaliski Jr et M. Robshaw,
"Linear Cryptanalysis Using Multiple Approximations of FEAL",
Fast Software Encryption, Second International Workshop Proceedings,
Springer-Verlag, 1995, pp. 249-264

6.19 Cryptanalyse de TWOPRIME

Lisez:

C. Ding, V. Niemi, A. Renvall et A. Salomaa,
"TWOPRIME: A Fast Stream Ciphering Algorithm",
Fast Software Encryption, 4th International Workshop Proceedings,
Springer-Verlag, 1997, pp. 88-102

TWOPRIME est réellement un chiffrement par blocs. Essayez de le briser; il y a toutes sortes d'attaques. Les résultats sont dans:

D. Coppersmith, D. Wagner, B. Schneier et J. Kelseym,
"Cryptanalysis of TWOPRIME",
Fast Software Encryption, 5th International Workshop Proceedings,
Springer-Verlag, 1998, pp. 32-48

6.20 Cryptanalyse de Blowfish

Lisez:

B. Schneier,
"Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)",
Fast Software Encryption, Cambridge Security Workshop Proceedings,
Springer-Verlag, 1994, pp. 191-204

Et essayez de briser Blowfish. Quelques résultats sont publiés dans:

S. Vaudenay, "On the Weak Keys in Blowfish",
Fast Software Encryption, 3rd International Workshop Proceedings,
Springer-Verlag, 1996, pp. 27-32

Il y a aussi une attaque différentielle contre un Blowfish à cinq rondes dans la thèse de V. Rijmen.

6.21 Cryptanalyse de ICE

Lisez:

M. Kwan, "The Design of ICE Encryption Algorithm",
Fast Software Encryption, 4th International Workshop Proceedings,
Springer-Verlag, 1997, pp. 69-82

Une attaque différentielle est dans:

B. Van Rompay, L.R. Knudsen et V. Rijmen,
"Differential Cryptanalysis of ICE Encryption Algorithm",
Fast Software Encryption, 5th International Workshop Proceedings,
Springer-Verlag, 1998, pp. 270-283

6.22 Cryptanalyse de LOKI-91

LOKI a été révisé; la nouvelle version s'appelle LOKI-91. Lisez:

L. Brown, M. Kwan, J. Pieprzyk et J. Seberry,
"Improving Resistance to Differential Cryptanalysis and the Redesign of LOKI",
Advances in Cryptology ASIACRYPT '91 Proceedings,
Springer-Verlag, 1993, pp. 36-50

Recherchez tout type de cryptanalyse; certains résultats peuvent être trouvés dans:

L.R. Knudsen, "Cryptanalysis of LOKI-91",
Advances in Cryptology AUSCRYPT '92,
Springer-Verlag, 1993, pp. 196-208

Une attaque linéaire (sur LOKI-91 et LOKI-89) peut être trouvée dans:

T. Tokita, T. Sorimachi et M. Matsui,
"Linear Cryptanalysis of LOKI and s^2DES",
Advances in Cryptology ASIACRYPT '94,
Springer-Verlag, 1995, pp. 293-303

6.23 Cryptanalyse de CMEA

Lisez les sections 1 et 2 de:

D. Wagner, B. Schneier et J. Kelsey,
"Cryptanalysis of the Cellular Message Encryption Algorithm",
Advances in Cryptology CRYPTO '97 Proceedings,
Springer-Verlag, 1997, pp. 526-537

Essayez de briser l'algorithme avant de lire le reste du document.

6.24 Cryptanalyse d'IDEA

IDEA est décrit (sous le nom de IPES) dans:

X. Lai, J. Massey et S. Murphy,
"Markov Ciphers and Differential Cryptanalysis",
Advances in Cryptology EUROCRYPT '91 Proceedings,
Springer-Verlag, 1991, pp. 17-38

L'analyse la plus facile est de rechercher les clefs faibles; une réponse se trouve dans:

J. Daemen, R. Govaerts et J. Vandewalle, "Weak Keys for IDEA",
Advances in Cryptology CRYPTO '93 Proceedings,
Springer-Verlag, 1994, pp. 224-231

Recherchez d'autres attaques; des solutions se trouvent dans:

W. Meier, "On the Security of the IDEA Block Cipher",
Advances in Cryptology EUROCRYPT '93 Proceedings,
Springer-Verlag, 1994, pp. 371-385

et dans:

P. Haawkes et L. O'Connor, "On Applying Linear Cryptanalysis to IDEA",
Advances in Cryptology ASIACRYPT '96,
Springer-Verlag, 1996, pp. 105-115

6.25 Différentielles tronquées

Lisez les sections 1 à 4 de:

L.R. Knudsen, "Truncated and Higher Order Differentials",
Fast Software Encryption, 2nd International Workshop Proceedings,
Springer-Verlag, 1995, pp. 196-211

Essayez d'appliquer les techniques des différentielles tronquées avant de lire les résultats dans la section 5. Essayez de briser SAFER en utilisant les différentielles tronquées. Les résultats sont dans:

L.R. Knudsen et T.A. Berson,
"Truncated Differentials of SAFER",
Fast Software Encryption, 3rd International Workshop Proceedings,
Springer-Verlag, 1996, pp. 15-26

6.26 Cryptanalyse différentielle à clef liées

Lisez:

J. Kelsey, B. Schneier et D. Wagner,
"Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER and Triple-DES",
Advances in Cryptology CRYPTO '96 Proceedings,
Springer-Verlag, 1996, pp. 237-251

Essayez d'appliquer les techniques à 3-Way, DES-X et TEA avant de lire:

J. Kelsey, B. Schneier et D. Wagner,
"Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2 and TEA",
Information and Communications Security,
First International Conference Proceedings,
Springer-Verlag, 1997, pp. 203-207

6.27 Généralisations de la cryptanalyse linéaire

Lisez:

C. Harpes, G. Kramer et J. Massey,
"A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-Up Lemma",
Advances in Cryptology EUROCRYPT '95 Proceedings,
Springer-Verlag, 1997, pp. 13-27

Essayez d'appliquer ces techniques au DES avant de lire l'appendice C du second document. Lisez les sections 1 à 4 de:

B. Kaliski Jr et M. Robshaw,
"Linear Cryptanalysis Using Multiples Approximations",
Advances in Cryptology CRYPTO '94 Proceedings,
Springer-Verlag, 1994, pp. 26-39

Essayez d'appliquer les techniques à LOKI-91 avant de lire la section 5.

6.28 Cryptanalyse d'Akelarre

Lisez:

G. Alvarez, D. De la Guia, F. Montoya et A. Peinado,
"Akelarre: A New Block Cipher Algorithm",
Workshop on Selected Areas in Cryptography (SAC '96) Workshop Record,
Queens University, 1996, pp. 1-4

Essayez de briser l'algorithme. Les résultats sont dans:

L.R. Knudsen et V. Rijmen, "Two Rights Sometimes Make a Wrong",
Workshop on Selected Areas in Cryptography (SAC '97) Workshop Record,
School of Computer Science, Carleton University, 1997, pp. 213-223

et:

N. Ferguson et B. Schneier, "Cryptanalysis of Akelarre",
Workshop on Selected Areas in Cryptography (SAC '97) Workshop Record,
School of Computer Science, Carleton University, 1997, pp. 201-212

Une description d'Akelarre est dans le dernier document, si vous ne trouvez pas les autres.

6.29 Blanchiement

Lisez:

J. Kilian et P. Rogaway, "How to Protect DES Against Exhaustive Key Search",
Advances in Cryptology CRYPTO '96 Proceedings,
Springer-Verlag, 1996, pp. 252-267

6.30 Théorie des cryptanalyses différentielles et linéaires

Lisez les documents suivants:

K. Nyberg, "Linear Approximation of Block Ciphers",
Advances in Cryptology EUROCRYPT '94 Proceedings,
Springer-Verlag, 1995, pp. 439-444

K. Nyberg et L. Knudsen, "Provable Security Against a Differential Attack", Journal of Cryptology, v.8, n.1, 1995, pp. 27-37

K. Nyberg et L. Knudsen, "Provable Security Against a Differential Cryptanalysis",
Advances in Cryptology CRYPTO '92 Proceedings,
Springer-Verlag, 1993, pp. 566-574

6.31 Cryptanalyse de VINO

Lisez:

A. Di Porto et W. Wolfowicz, "VINO: A Block Cipher Including Variable Permutations",
Fast Software Encryption, Cambridge Security Workshop Proceedings,
Springer-Verlag, 1994, pp. 205-210

Aucune cryptanalyse n'a été publiée: essayez d'être le premier.

6.32 Attaque d'interpolation

Lisez les sections 1 à 3.3 de:

T. Jakobsen et L. Knudsen, "The Interpolation Attack on Block Ciphers",
Fast Software Encryption, 4th International Workshop Proceedings,
Springler-Verlag, 1997, pp. 28-40

Lisez les modifications apportées à SHARK dans la section 3.4 et essayez de le briser avant de lire le reste du document.

6.33 Attaques des fonctions de rondes non-subjectives

Lisez:

E. Biham et A. Biryukov, "An Improvement of Davie's Attack on DES",
Advances in Cryptology EUROCRYPT '94 Proceedings,
Springer-Verlag, 1995, pp. 461-467

Une bonne lecture est aussi:

B. Rijmen, B. Preneel et E. De Win,
"On Weaknesses of Non-subjective Round Functions",
Designs, Codes, and Cryptography, v.12, n.3, 1997, pp. 253-266

6.34 Cryptanalyse de Khufu

Lisez la description de Khufu dans:

R.C. Merkle, "Fast Software Encryption Functions",
Advances in Cryptology CRYPTO '90 Proceedings,
Springer-Verlag, 1991, pp. 476-501

Essayez de le briser. Une analyse se trouve dans:

H. Gilbert et P. Chauvaud,
"A Choosen-Plaintext Attack on the 16-Round Khufu Cryptosystem",
Advances in Cryptology CRYPTO '94 Proceedings,
Springer-Verlag, 1994, pp. 359-368

6.35 Cryptanalyse de SAFER

Lisez:

J. L. Massey,
"SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm",
Fast Software Encryption, Cambridge Security Workshop Proceedings,
Springer-Verlag, 1994, pp. 1-17

Essayez d'attaquer le chiffrement. Des résultats peuvent être trouvés dans:

J. L. Massey, "SAFER K-64: One Year Later",
Fast Software Encryption, 2nd International Workshop Proceedings,
Springer-Verlag, 1995, pp. 212-241

S. Vaudenay, "On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER",
Fast Software Encryption, Second International Workshop Proceedings,
Springer-Verlag, 1995, pp. 286-297

et L.R. Knudsen, "A Key-Schedule Weakness in SAFER K-64",
Advances in Cryptology CRYPTO '95 Proceedings,
Springer-Verlag, 1995, pp. 274-286

6.36 Modes de fonctionnement

Lisez:

E. Biham, "On Modes of Operation",
Fast Software Encryption, Cambridge Security Workshop Proceedings,
Springer-Verlag, 1994, pp. 116-120

et:

E. Biham, "Cryptanalysis of Multiple Modes of Operation",
Advances in Cryptology ASIACRYPT '94 Proceedings,
Springer-Verlag, 1995, pp. 278-292

Lisez les sections 1 et 2 de:

E. Biham, "Cryptanalysis of Ladder-DES",
Fast Software Encryption, 4th International Workshop Proceeedings,
Springer-Verlag, 1997, pp. 134-138

Essayez de briser la construction avant de poursuivre votre lecture. Lisez aussi:

D. Wagner, "Analysis of Some Recently Proposed Modes of Operation",
Fast Software Encryption, 5th International Workshop Proceedings,
Springer-Verlag, 1998, pp. 254-269

et essayez de briser les constructions avant de lire l'analyse.

6.37 Cryptanalyse avancée d'IDEA

Essayez de briser l'IDEA en utilisant les différentielles tronquées et les caractéristiques différentielles-linéaires. Les résultats sont dans:

J. Borst, L.R. Knudsen et V. Rijmen,
"Two Attacks on Reduced IDEA",
Advances in Cryptology EUROCRYPT '97,
Springer-Verlag, 1997, pp. 1-13

et:

P. Hawkes, "Differential-Linear Weak Key Classes of IDEA",
Advances of Cryptology EUROCRYPT '98 Proceedings,
Springer-Verlag, 1998, pp. 112-126

6.38 Cryptanalyse de TEA

Lisez:

D. Wheeler et R. Needham, "TEA, a Tiny Encryption Algorithm",
Fast Software Encryption, 2nd International Workshop Proceedings,
Springer-Verlag, 1995, pp. 363-366

Aucune cryptanalyse, hormis sur la préparation de la clef, n'a été publiée: essayez d'être le premier.

6.39 Cryptanalyse de RC5

Lisez:

R.L. Rivest, "The RC5 Encryption Algorithm",
Fast Software Encryption, 2nd International Workshop Proceedings,
Springer-Verlag, 1995, pp. 86-96

Essayez de briser le RC5. Vous trouverez quelques résultats dans:

B.S. Kaliski et Y.L. Yin,
"On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm",
Advances in Cryptology CRYPTO '96 Proceedings,
Springer-Verlag, 1996, pp. 445-454

L.R. Knudsen et W. Meier, "Improved Differential Attacks on RC5",
Advances in Cryptology CRYPTO '96 Proceedings,
Springer-Verlag, 1996, 216-228

A.A. Selcuk, "New Results in Linear Cryptanalisys of RC5",
Fast Software Encryption, 5th International Workshop Proceedings,
Springer-Verlag, 1998, pp. 1-16

6.40 Cryptanalyse de MISTY

Lisez:

M. Matsui,
"New Structure of Block Ciphers with Provable Security Against Differential and Linear Cryptanalysis",
Fast Software Encryption, 3rd International Workshop Proceedings,
Springer-Verlag, 1996, pp. 205-218

M. Matsui, "New Block Encryption Algorithm MISTY",
Fast Software Encryption, 4th International Workshop Proceedings,
Springer-Verlag, 1997, pp. 54-68

Le seul résultat cryptanalytique publié que je connais est japonais:

H. Tanaka, K. Hisamatsu et T. Kaneko,
"High Order Attack of MISTY without FL Functions",
The Institute of Electronics, Information and Communications Engineers,
ISEC98-5, 1998.

6.41 Cryptanalyse de Square

Lisez:

J. Daemen, L. Knudsen et V. Rijmen, "The Block Cipher Square",
Fast Software Encryption, 4th International Workshop Proceedings,
Springer-Verlag, 1997, pp. 149-165

excepté la section 6: essayez d'attaquer le chiffrement avant de la lire.

6.42 Propositions à l'AES

En 1998, le National Institute of Standards and Technology a demandé des candidats afin de remplacer le chiffrement par blocs DES. Quinze propositions ont été reçues. Vous pouvez consulter l'évolution et le traitement des propositions à l'AES sur le site Internet du NIST, qui inclut des détails sur les diverses propositions: http://www.nist.gov/aes/

Cassez ce que vous pouvez, et envoyez les résultats au NIST.

7 Conclusion

Le seul moyen pour devenir un bon concepteur d'algorithmes est d'être un bon cryptanalyste: casser des algorithmes. Beaucoup. Encore et encore. Seulement après qu'un étudiant ait démontré ses capacités à cryptanalyser les algorithmes des autres, il pourra voir ses propres conceptions considérées sérieusement par les mêmes autres.

Étant donné que beaucoup de nouveaux algorithmes ont été créés ces dernières années certains publiés, certains brevetés, d'autres propriétaires comment font les cryptanalystes pour déterminer ceux qu'ils doivent continuer à étudier? Ils observent le pedigree de l'algorithme. Un algorithme qui a été inventé par quelqu'un qui a montré qu'il peut briser des algorithmes il aura étudié la littérature, peut-être en utilisant ce cours, et publié quelques faits qui n'auront pas été découverts avant lui a plus de chances d'inventer un chiffrement sûr, qu'une personne qui n'a fait que lire les documents disponibles, et qui a inventé son propre algorithme. Dans les deux cas, le créateur de l'algorithme est convaincu que son algorithme est sûr; dans le premier cas, l'opinion de l'auteur aura une valeur.

Les cryptanalystes font aussi attention à la documentation associée à la conception. A nouveau, la conception est facile, et l'analyse est difficile. Les conceptions qui sont fournies avec des analyses poussées des variantes simplifiées cassées, des versions à rondes réduites cassées, et des implémentations alternatives montrent que le créateur sait ce qu'il a fait quand il a créé son algorithme. Une simple étude des soumissions à l'AES révèle quelles conceptions ont été sérieusement préparées, et lesquelles ne l'ont pas été; une conception sérieuse c'est donc avant tout de la cryptanalyse.

Tout le monde peut inventer un algorithme qu'il ne pourra pas briser. Ce n'est même pas difficile. Ce qui est difficile c'est la cryptanalyse. Et seul un cryptanalyste expérimenté pourra concevoir un bon chiffrement.