Hücresel Otomata ve Kaos Tabanlı Bir Şifreleme Algoritmasının Güvenlik Analizi

Fatih Özkaynak, Ahmet Bedri Özer, Sırma Yavuz

***Özet*—Kriptolojik sistemlerin tasarımında kaos teorisinin iyi bir uygulama alanı olmasına rağmen birçok uygulama güvenli iletişim için yetersiz kalmaktadır. Çünkü kriptanaliz çalışmaları yetersizdir. Zayıf önerilerin ortaya çıkmasındaki en önemli sebep şifreleme algoritmalarının güvenlik analizinin sadece istatistiki testler ve deneysel sonuçlar ile yapılmasıdır. Machicao ve arkadaşları bir şifreleme algoritması önermişlerdir. Önerilen şifreleme algoritmasının güvenlik analizleri sadece istatistiksel testler kullanılarak yapılmıştır. Bu çalışmada önerilen algoritmanın güvenlik zayıflıkları analiz edilmiştir. Önerilen algoritma için iki farklı saldırı gerçekleştirilmiştir. İlk saldırıda şifreleme algoritmasının gizli anahtarı sadece bir açık/şifreli veri çifti kullanılarak nasıl elde edilebileceği gösterilmiştir. İkinci saldırıda sözde rasgele üretecin çekirdek değerleri kullanılarak lojistik haritanın anahtar uzayının nasıl indirgenebileceği gösterilmiştir. Bu saldırı ile tüm olası çekirdek değerleri açığa çıkarılmıştır.**

***Anahtar Kelimeler*— Kaos; Kriptoloji; Hücresel otomata; Kriptanaliz**

***Abstract*— Although chaos theory is a good application field in the design of cryptographic systems, many proposals become unsatisfactory for secure communication since cryptanalysis studies are not sufficient. One of the important factors resulting in poor proposals is the fact that security analysis of the encryption algorithms is performed with only statistical tests and experimental results. An encryption algorithm was proposed by Machicao et al. Security analyses of the proposed encryption algorithm were done only by using statistical tests. In this study, we analyze the security weaknesses of the proposed algorithm. Two different attacks have been carried out for proposed algorithm. The first attack has shown that how to obtain the secret key of encryption algorithm using only one plaintext/ciphertext pairs. The second attack has shown that how to reduce key space of logistic map, which is used in seed values for pseudo random generator. All possible seed values have been revealed with this attack.**

***Index Terms*— Chaos; Cryptography; Cellular automata; Cryptanalysis**

I. GİRİŞ

AĞ ve iletişim teknolojilerindeki hızlı gelişmeler ile birlikte günlük yaşantımız büyük ölçüde sayısallaşmıştır. Sayısal ortamlarda kritik öneme sahip verilerin işlenmesi, depolanması ve iletilmesi ile bu verilerin güvenliğinin nasıl sağlanacağı sorusunu ön plana çıkarmıştır [1]. Araştırmacılar güvenlik problemini çözebilmek için geleneksel kriptolojik çözümlere alternatif olabilecek etkili, hızlı ve gürbüz algoritmalar geliştirme arayışı içerisine girmiştir. Bu doğrultuda kaos tabanlı kriptoloji çalışmaları da son yirmi yılda önemli bir ilgi odağı olmuştur [2-8].

Kaotik sistemlerin doğrusal olmaması, gürültü benzeri periyodik olmayan bir davranış göstermesi ve başlangıç koşullarına hassas duyarlılığı gibi özellikleri kullanılarak kriptolojik protokollerin tasarlanması birçok araştırmacının ilgisini çekmiştir. Ancak protokollerin analiz çalışmaları ve kriptolojik tasarım süreci yeterince irdelenmediğinden birçok önerinin basit bilinen saldırılara karşı zayıf olduğu gösterilmiştir [9-17].

Machicao ve arkadaşları [18] hücresel otomatanın kaotik davranış göstermesinden yola çıkarak yeni bir kaos tabanlı şifreleme algoritması önermişlerdir. Önerilen yöntemin güvenlik analizleri çeşitli istatistiki testler ile yapılmıştır. İstatistiki analizler sonucunda önceki önerilere göre daha iyi sonuçlar elde edilmiştir. Ancak istatistiki testler bir şifreleme algoritmasının sağlaması gereken unsurlardan biri olmasına rağmen tek başına yeterli değildir.

Bu çalışmada Machicao ve arkadaşları tarafından önerilen algoritmanın detaylı güvenlik analizleri yapılmıştır. İlk saldırıda; sadece bir adet açık/şifreli veri çifti kullanılarak şifreleme algoritmasının gizli anahtarının nasıl elde edilebileceği gösterilmiştir. İkinci saldırıda ise algoritmada rasgele sayı üreteci için çekirdek değerleri üretmede kullanılan lojistik haritanın anahtar uzayının nasıl indirgeneceği gösterilmiştir. Bu saldırı ile üretilebilecek olası bütün çekirdek değerleri açığa çıkarılmıştır. Yapılan analiz çalışmaları sonucunda önerilen yöntemin güvenli iletişim için uygun olmadığı gösterilmiştir.

Çalışmanın geri kalan kısmı aşağıdaki gibi organize edilmiştir. İkinci bölümde analiz edilen algoritmanın yapısı kısaca özetlenmiştir. Üçüncü bölümde analiz edilen algoritmaya yapılan saldırıların mantığı açıklanmıştır. Son bölümde elde edilen sonuçlar tartışılmıştır.

II. ALGORİTMANIN YAPISI

Machicao ve arkadaşları kabaca şekil 1'de gösterildiği gibi bir blok şifreleme algoritması önermişlerdir [18]. Algoritmada her bir blok şifrelenirken anahtar ve kendinden önce şifrelenen blok kullanılmaktadır. Algoritmanın matematiksel gösterimi Denklem 1 ve Denklem 2'de verilmiştir. Önerilen algoritmanın yeniliği ise her bir bloğun şifrelenmesinde kullanılan anahtarların üretim mantığında gizlidir. Machicao ve arkadaşları anahtar üretimi için üç

Fatih Özkaynak, Fırat Üniversitesi Yazılım Mühendisliği Bölümü 23119 Elazığ Türkiye (iletişim yazarı tel: 424-2370000/4241; e-posta: ozkaynak_fatih@hotmail.com).

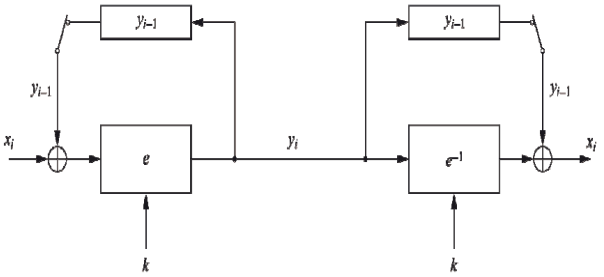
Ahmet Bedri Özer, Fırat Üniversitesi Bilgisayar Mühendisliği Bölümü 23119 Elazığ Türkiye (e-posta: bedriozer@firat.edu.tr).

Sırma Yavuz, Yıldız Teknik Üniversitesi Bilgisayar Mühendisliği Bölümü 343349 İstanbul Türkiye (e-posta: sirma@ce.yildiz.edu.tr).

aşamalı bir yöntem kullanmışlardır. Her bir aşamada gerçekleştirilen işlemlerin listesi aşağıda adım adım verilmiştir.

$$y_1 = k_1 \oplus x_1 \quad (1)$$

$$y_i = k_i \oplus x_i \oplus y_{i-1}, \quad i > 1 \quad (2)$$



Şekil 1. Şifreleme algoritmasının genel yapısı

Birinci aşama içerinde yapılan işlemler

1. Şifreleme algoritmasının gizli anahtarı olarak 128 bit uzunluğunda bir değer belirlenir.
2. Denklem 3, 4 ve 5 kullanılarak π gizli anahtarından kaotik sistemin başlangıç koşulu x_0 belirlenir.

$$\Omega := \sum_{i=1}^{size(\vec{\pi})} 2^{8*(i-1)} \pi_i \quad (3)$$

$$\Omega = \frac{\Omega}{2^{(8*size(\vec{\pi})+1)}} \quad (4)$$

$$X_0 = \Omega + 0.00001 \quad (5)$$

3. Lojistik harita itere edilir. İlk 1000 iterasyon geçici etkilerin ortadan kalkması için alınmaz.
4. Denklem 6'da verilen niceleme mantığı kullanılarak [0, 1] aralığında üretilen sürekli değerler binary değerlere ayrıklaştırılır.

$$\begin{cases} 1 & if\ X_k < 0.5 \\ 0 & if\ X_k \geq 0.5 \end{cases} \quad (6)$$

5. Lojistik haritanın iterasyonları sonucunda m×n boyutunda binary bir dizi üretilir.

İkinci aşama içerisinde yapılan işlemler

1. m×n boyutundaki binary dizi hücresel otomatın başlangıç değerleri olarak atanır.
2. Doğal hücresel olguları modellemede kullanılan "Gam-of-Life" kuralları kullanılarak yeni jenerasyonlar üretilir. Farklı kuralların kullanılması farklı jenerasyonların elde edilmesine sebep olmaktadır. Detaylar için kaynak [18] incelenebilir.
3. Şifreleme algoritmasında yeni popülasyonların üretilmesi için 64×64 boyutunda bir hücresel otomata ve B1357/S2468 kuralı kullanılmıştır

Üçüncü aşama içerisinde yapılan işlemler

1. 64×64 boyutundaki hücresel otomat bloklara ayrılır.
2. Elde edilen bloklara XOR işlemi uygulanarak her bir bloğun şifrelenmesinde kullanılacak anahtar değeri üretilir.

Anahtar değerinin üretilmesinin ardından Denklem 1 ve Denklem 2'de verilen yapı kullanılarak her bir bloğun şifrelenmesi işlemi gerçekleştirilir.

III. Güvenlik Analizi

A. *Saldırı Senaryosu 1*

Şifreleme sistemlerinin temel gereksinimleri olan karıştırma ve yayılma özelliklerini sağlamak için; doğrusal olmayan dinamikler, kaos, DNA işlemleri ve hücresel otomatlar gibi yapıların teorik olarak zengin dinamikler sunması birçok araştırmacıyı bu konuda çalışmaya yönlendirmiştir. Ancak araştırmacıların genel eğilimi bu yapıları farklı tasarımlarda değişik biçimde kullanarak yeni şifreleme sistemleri geliştirme yönünde olmuştur. Buda kriptolojik tasarım sürecinin gözden kaçırılmasına ve birçok bilinen basit saldırıya karşı zayıf önerilerin ortaya çıkmasına sebep olmuştur [19, 20].

Machicao ve arkadaşları da kaos, hücresel otomata ve Game-of-Life süreçlerini kullanarak şifreleme algoritmasının her bir bloğunda kullanılmak üzere bir anahtar üreteci tasarlamışlardır. Üretilen anahtarlar istatistiki olarak birçok rasgelelik testini geçmesine rağmen şifreleme siteminin cebirsel bağımlılıklar içermesi sonucunda sadece bir adet açık/şifreli veri çiftinin bilinmesi durumunda anahtar değeri elde edilebileceği gösterilmiştir. Denklem 1 ve Denklem 2'de genel yapısı verilen şifreleme algoritması daha açık biçimde Denklem 7'deki gibi yazılabilir. Denklem 7'de XOR işleminin birleşme özelliği kullanılarak yeniden düzenlenirse Denklem 8'deki gibi şifreleme algoritmasının daha basit bir ifadesi ortaya çıkmaktadır.

$$y_i = k_i \oplus x_i \oplus k_{i-1} \oplus x_{i-1} \oplus \ldots \oplus k_2 \oplus x_2 \oplus k_1 \oplus x_1 \quad (7)$$

$$y_i = (k_i \oplus k_{i-1} \oplus \ldots \oplus k_2 \oplus k_1) \oplus (x_i \oplus x_{i-1} \oplus \ldots \oplus x_2 \oplus x_1) \quad (8)$$

En basit saldırı yöntemlerinden biri bilinen açık metin saldırısıdır. Bu saldırıda, saldırgan özel seçtiği bir açık metine karşılık gelen şifreli metni bulur. Açık/şifreli veri çiftlerini kullanarak algoritmanın gizli parametresi olan anahtarı elde etmeye çalışır. Denklem 8'de elde edilen yapı için açık/şifreli veri çiftleri denklemde yerine yazılırsa algoritmanın gizli parametresi olan anahtar değerleri açığa çıkarılmış olur. Anahtar değerine sahip olan bir kişi istediği herhangi bir veriyi şifreleyebilir veya şifresini çözebilir.

Saldırı sonucunda görülmüştür ki; şifreleme algoritması içerisinde kullanılan yapıların kriptolojik olarak güçlü karakteristiklere sahip olması gerekmektedir. Ancak ne kadar güçlü yapılar kullanılırsa kullanılsın asıl önemli olan bu yapıların kriptolojik tasarım sürecinde nasıl kullanıldığıdır.

B. *Saldırı Senaryosu 2*

Kerckhoffs prensibine göre bir şifreleme algoritmasında anahtar dışında her şey açık olmalıdır. n-bitlik gizli anahtara

sahip bir şifreleme algoritmasında anahtar uzayı 2^n'dir. Anahtar uzayındaki olası bütün anahtarların denenmesi ile yapılan saldırı kaba kuvvet saldırısı olarak adlandırılmaktadır. Modern şifreleme algoritmaları için 128-bitlik anahtar uzunluğu kaba kuvvet saldırısını önlemektedir. Analiz edilen algoritmanın anahtar boyu 128-bit olarak belirlendiği için kaba kuvvet saldırısı mantıksızdır [21, 22].

Kriptanalistin amacı kaba kuvvet saldırısından daha az hesaplama maliyetine sahip bir yöntem olup olmadığının araştırılmasıdır. Algoritmada gizli anahtar Denklem 3, 4 ve 5'de gösterildiği gibi lojistik haritanın başlangıç koşullarının belirlenmesinde kullanılmıştır. Gizli anahtar boyutu 128-bit olduğu için lojistik haritanın başlangıç koşulu olarak 2^128 farklı durum söz konusudur. Kaotik sistemler başlangıç koşullarına hassas duyarlı olduğu için teorik olarak 2^128 farklı başlangıç koşulu için 2^128 farklı yörünge elde edilmesi gerekmektedir. Ancak pratik uygulamalar göz önüne alındığında hesaplama duyarlılığına bağlı olarak anahtar uzayının tahmin edilenden daha kısa olduğu bu saldırıda gösterilmiştir.

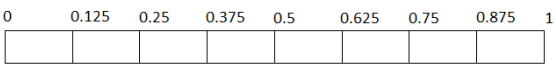
Lojistik harita [0,1] aralığında sürekli değerler almaktadır. Ancak hesaplamaların yapıldığı makinanın hesaplama duyarlılığına bağlı olarak bir sayısal kötüleşme meydana gelmektedir. Hesaplamalarda virgülden sonraki k dijit kullanılıyorsa (k+1). dijit için bir yuvarlama hatası meydana gelecektir. Örneğin hesaplama duyarlılığının virgülden sonraki 3 dijit kullanılarak yapıldığını varsayalım. Olası başlangıç değerlerinin sayısı 2^3=8'dir. Ancak teoride olası başlangıç değerlerinin sayısı n>8 olduğu için güvercin deliği prensibine göre bu başlangıç değerlerinden üretilen yörüngelerde bir çakışma meydana gelecektir. Önerilen saldırı senaryosunun temeli de bu sayısal kötüleşmeden dolayı yörüngelerin birbiriyle çakışmasına ve olası anahtar uzayının teorik hesaplamalardan daha düşük olduğunun gösterilmesine dayanmaktadır.

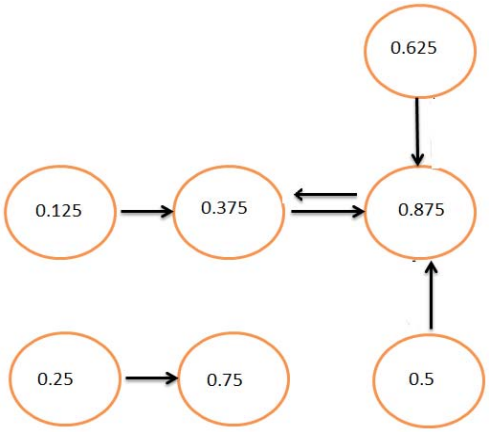
Şekil 2'de 3 bit duyarlılığa sahip bir makine üzerinde lojistik haritanın yörüngelerinin değişimi gösterilmiştir. Şekil 2.(a)'da [0, 1] aralığı 2^3=8 parçaya bölünerek aralıkların alt ve üst limitleri belirlenmiştir. Ardından her bir aralık başlangıç değeri olarak Denklem 9'da verilen lojistik harita için kullanılmış ve çıkış değeri elde edilmiştir. Elde edilen çıkış değeri hangi aralığa denk geliyorsa çıkış değeri o aralığa yuvarlanmıştır. Periyodik bir çevrim bulununcaya kadar iterasyonlara devam edilmiştir.

Örneğin x_0=0.125 başlangıç koşulu için denklem 9 çalıştırılırsa x_1=0.4375 olarak hesaplanmaktadır. Bu değer hesaplama duyarlılığına bağlı olarak 0.375 olarak alınmaktadır. 0.375 değeri için x_2=0.9375 olarak hesaplanır. x_2 değeri de hesaplama duyarlılığına bağlı olarak 0.875 olarak alınmaktadır. 0.875 değeri kullanılarak x_3 değeri hesaplanırsa bir çevrim bulunur.

$$X_{k+1} = 4 * X_k * (1 - X_k) \quad (9)$$

Şekil 2 3-bit hesaplama duyarlılığı için yörüngelerin değişimi gösterilmiştir.





Şekil 2 3-bit hesaplama duyarlılığı için yörüngelerin değişimi

Şekil 2'den görülebileceği gibi teorik olarak 8 farklı başlangıç durumu için 8 farklı yörünge oluşması beklenirken 3 bit hesaplama duyarlılığı için sadece 2 farklı yörünge elde edildiği görülmektedir. Çalışmada gösterim basit olması açısından 3-bit hesaplama duyarlılığı seçilmiştir. Hesaplama hassasiyetinin arttırılmasıyla birlikte farklı yörüngelerin sayısının atması beklenirken bu işlemin her zaman için geçerli olmadığı deneysel sonuçlarla gösterilmiştir. Örneğin hesaplama duyarlılığı 5-bit seçildiğinde maksimum uzunluklu periyot çevrimi 8 iken hesaplama duyarlılığın 6'ya çıkarıldığında maksimum uzunluklu periyot çevriminin 7 olduğu gözlemlenmiştir.

Lojistik haritanın yörüngelerinin çakışması sonucunda hücresel otomatatın başlangıç değerleri aynı olacaktır. Aynı değerler aynı anahtları üreteceğinden anahtar uzayında bir daralma meydana gelecektir. Buda kaba kuvvet saldırılarını mümkün kılacaktır.

IV. SONUÇLAR

Kaos ve kriptoloji bilimleri benzer özellikler göstermesinden dolayı aralarında güçlü bir bağlantı vardır. Ancak iki disiplin arasındaki benzerliklerin yanı sıra farklılıklarda detaylı olarak irdelenmelidir. İki disiplin arasındaki en dikkat çekici ayrımlardan biri kaotik sistemlerin faz uzayının reel sayılar üzerinde tanımlı olmasına rağmen kriptolojik sistemlerin tam sayıların bir kümesini temel alarak tasarlanmasıdır. Dolayısıyla kaotik sistemler kriptolojik uygulamalarda kullanılacaksa bir ayrıklaştırma işlemine gereksinim duyulmaktadır. Ayrıklaştırma işlemi sonucunda bir sayısal kötüleşme meydana geleceği hem teorik hem de pratik olarak bilinmektedir. Sonuç olarak kaotik sistemler yeni kriptolojik sistemlerin tasarımında kullanılacaksa sayısal kötüleşmenin etkileri iyi incelenmelidir. Bu çalışmada hesaplama duyarlılığına bağlı olarak sayısal kötüleşmeden dolayı olası anahtar uzayının teorik hesaplamaların altında olduğu ve bu değerin güvenli iletişim için uygun olmadığı gösterilmiştir.

Çalışmada gösterilen diğer bir saldırı ise şifreleme algoritmasının cebirsel bağımlılıklar içermesidir. Bu sadece kaos tabanlı kriptolojik tasarımlar için değil genel olarak dikkat edilmesi gereken bir konudur. Çünkü kriptanalist bir sistemi analiz ederken tasarımda çok güçlü kriptolojik

elemanların kullanılmasıyla ilgilenmez. Kriptanalistin asıl hedefi elemanların kullanım biçimindeki zayıflıkları ortaya çıkarmak olduğu unutulmamalıdır.

KAYNAKLAR

[1] Katz, J., Lindell, Y., (2008). Introduction to modern cryptography: principles and protocols, Chapman & Hall.

[2] Alvarez, G., Li, S., (2006). Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos, 16/8, 2129–2151.

[3] Amigo, J. M., Kocarev, L., Szczapanski, J., (2007). Theory and practice of chaotic cryptography, Physics Letters A, 366, 211-216.

[4] Fridrich, J., (1998). Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos, 8/6, 1259–1284.

[5] Patidar, V., Pareek, N.K., Sud, K.K., (2009). A new substitution-diffusion based image cipher using chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulation, 14/7, 3056–3075.

[6] Liu, L., Zhang, Q., Wei, X., (2012). A RGB image encryption algorithm based on DNA encoding and chaos map, Computers & Electrical Engineering, 38/5, 1240-1248.

[7] Zhu, C., (2012). A novel image encryption scheme based on improved hyperchaotic sequences, Optics Communications, 285/1, 29-37.

[8] Hu, H., Liu, L., Ding, N., (2013). Pseudorandom sequence generator based on Chen chaotic system, Computer Physics Communications 184 (3) 765–768

[9] Özkaynak, F., Özer, A. B., Yavuz, S., (2012). Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences, Optics Communications, 285, 4946–4948.

[10] Rhouma, R., Solak, E., Belghith, S., (2010). Cryptanalysis of a new substitution–diffusion based image cipher, Communications in Nonlinear Science and Numerical Simulation, 15/7, 1887-1892.

[11] Solak, E., Çokal, C., Yildiz, O.T., Biyikoglu, T., (2010). Cryptanalysis of fridrich's chaotic image encryption, International Journal of Bifurcation and Chaos, 20/5, 1405–1413.

[12] Özkaynak, F., Özer, A. B., Yavuz, S., (2012). Cryptanalysis of Bigdeli algorithm using Çokal and Solak attack, International Journal of Information Security Science, 1/3, 79-81.

[13] Özkaynak, F., Özer, A. B., Yavuz S., (2013). Security problems of pseudorandom sequence generator based on Chen chaotic system, Computer Physics Communications 184, 2178–2181.

[14] Özkaynak, F., Özer, A. B., Yavuz S., (2013). Security Analysis of An Image Encryption Algorithm Based on Chaos and DNA Encoding, 21th IEEE Signal Processing and Communications Applications Conference, Cyprus.

[15] Özkaynak, F., Özer, A. B., Yavuz S., (2013). Kriptolojik Uygulamalarda İstatistiki Rasgelelik Testlerinin Problemleri, Kripto Günleri, Bilgem/Tübitak.

[16] Özkaynak, F., Özer, A. B., Yavuz S., (2012). Differential Cryptanalysis of Block Ciphers Based on Randomly Selected Substitution Boxes, 5th International Conference on Information Security and Cryptology, Ankara, Turkey

[17] Özkaynak, F., Özer, A. B., Yavuz S., (2012). Analysis of Chaotic Methods for Compression and Encryption Processes in Data Communication, 20th IEEE Signal Processing and Communications Applications Conference, Muğla, Turkey.

[18] Machicao, J., Marco, A. G., Bruno, O. M., (2012). Chaotic encryption method based on life-like cellular automata, Expert Systems with Applications, 39/16, 12626–12635.

[19] Alvarez, G., Amigo, J. M., Arroyo, D., Li, S., (2011). Lessons Learnt from the Cryptanalysis of Chaos-Based Ciphers. In: L. Kocarev, S. Lian (Eds.), Chaos Based Cryptography Theory Algorithms and Applications (pp. 257-295). Springer-Verlag.

[20] Solak, E., (2011). Cryptanalysis of Chaotic Ciphers. In: L. Kocarev, S. Lian (Eds.), Chaos Based Cryptography Theory Algorithms and Applications (pp. 227-256). Springer-Verlag.

[21] Bard, G. V., (2009). Algebraic Cryptanalysis, Springer

[22] Joux, A., (2009). Algorithmic cryptanalysis, Chapman & Hall.