Advances in Engineering Research (AER), volume 124
2nd International Symposium on Advances in Electrical, Electronics and Computer Engineering
(ISAEECE 2017)

Attacks and Defenses in Cryptography

Xiaoling Zhu[1, a] and Zhengfeng Hou[1,b]

[1] School of Computer and Information, Hefei University of Technology, Hefei 230009, China

[a]zhuxl@hfut.edu.cn, [b]houzf@hfut.edu.cn

Keywords: Cryptography; Attack and defense framework; Implementation cases

Abstract. Attacks and defenses have always been the focus of information security. If some new attacks appear, the corresponding defense methods will be proposed. In particular, cryptography, as a key security technology, has developed in such an offensive and defensive confrontation environment. For classical cryptography and modern cryptography, attack models, attack means, security models, and security properties are given. Furthermore, attack and defense cases are demonstrated to provide a reference for enhancing the security of cryptography algorithms.

Introduction

In the face of ubiquitous security threats in cyberspace, active and professional defenses are essential. During the defense-attack-defense process, security technology has entered a healthy state of spiral rising and system security has increasingly been improved. Also, the attack and defense confrontation, as a main line, runs through the development of cryptography all the time and becomes the important content in cryptography.

Cryptography was traced back to Kaiser cipher in the ancient Rome era, and then the affine cipher. The substitution cipher extends the key space greatly in order to resist a brute attack; but using frequency analysis method, it is cracked easily. Virginia cipher is one type of polyalphabetic substitution ciphers, once considered unbreakable. When facing Kasisk test and the coincidence index method, it was cracked. Enigma was used by Hitler in the World War II. In order to crack Enigma, Alan Turing created the first computer. Since then, cryptography bid farewell to classical cryptography and entered modern cryptography. Data encryption standard (DES) was a milestone; differential analysis, linear analysis, and other new analysis methods were provided. To resist the analysis methods, the advanced encryption standard (AES) was designed. But the problem of key distribution was still difficult to solve. The new idea of public key cryptography happened, and RSA was put forward. Later, the elliptic curve, identity, quantum and other cryptography methods continue to emerge, and their anti-attack capability is increasingly strong.

Attack and Defense in Classical Cryptography

First, the general attack models are given. Then for the existing cryptography algorithms, the attack means are discussed [1].

A. Theoretical Framework of Classical Cryptography. The attack and defense framework of classical cryptography is shown in Fig.1. The attack models include [2] only cipher text attack (COA), known plaintext attack (KPA), CPA (chosen plaintext attack) and CCA (chosen cipher text attack). The models describe different attack scenarios and attack capabilities. When a key space is small, an exhaustion search is effective. For simple single table substitution ciphers, such as Caesar and the affine cipher, they are cracked by an exhaustion search. Frequency analysis uses the cipher characters with significant statistical characteristics as a breakthrough to obtain the key, and it is often used in code breaking. Under KPA, Hill cipher and the LFSR stream cipher are cracked by solving a modular linear equation.

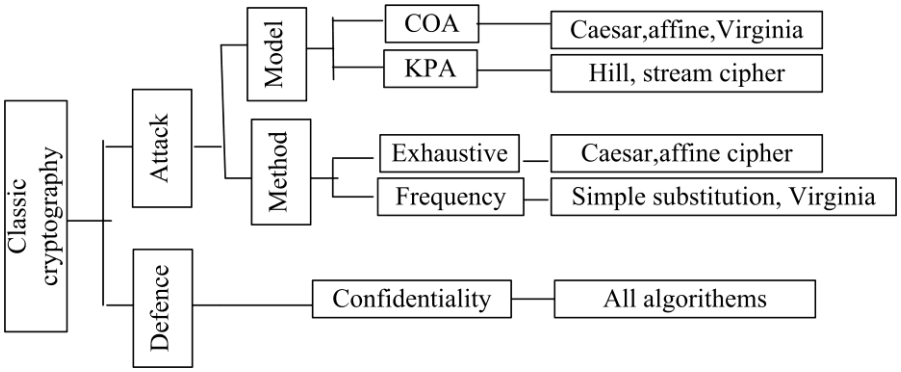
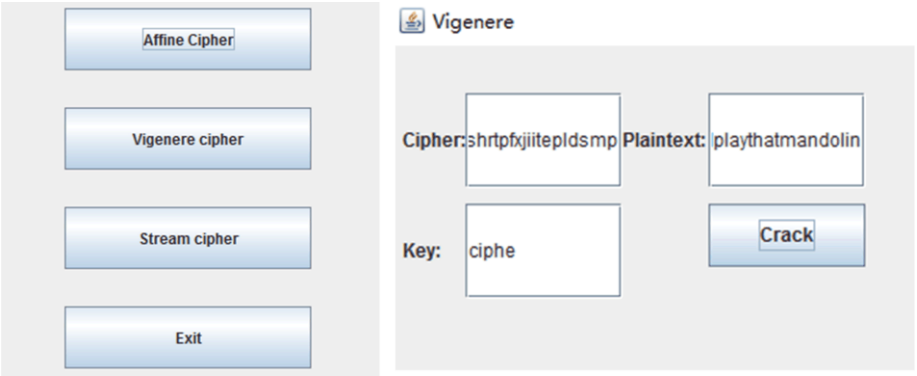


Fig.1. Attack and defense framework of classical cryptography

B. Practice Cases in Classical Cryptography. Fig.2(a) shows the interactive interface for encryption and decryption of the affine cipher, Viginier cipher and stream cipher. As for code breaking of Hill and Vigenere, when their ciphers are given, find out their possible plaintexts and keys. For Hill and LFSR, when their plaintext-ciphertext pairs are given, find out their possible keys. In particular, Fig.2(b) shows the code breaking results of Vigenere using the coincidence index method.



(a) (b)

Fig.2. (a) Encryption, decryption and (b) code breaking in classical cryptography

Attack and Defense in Modern Cryptography

A. Theoretical Framework of Modern Cryptography. Fig.3 shows the models and methods of attack and defense in modern cryptography. Time and space compromise [3], collision attack, factorization, and computation of discrete logarithm are all common attack methods. In the middle meet attack on 2DES with 112 bit keys, the time decreased from 2^{112} to 2^{56} through storing $2*2^{56}$ temporary ciphertexts. This attack can be avoided in the 3DES. Under CPA, differential analysis obtains the partial keys based on differential relationship with high probability. Under KPA, linear analysis obtains the partial keys based on linear relationship with obvious bias. The two attacks require a large number of plaintext-ciphertext pairs; in most cases, they are impractical. Based on the birthday attack, a collision attack tries $2^{l/2}$ times hash computation to find a collision at least 1/2 probability. Because the security base of RSA and Rabin is the problem of large integer factorization, factorization could crack RSA and Rabin; the effective factorization algorithms are Pollard p-1, Pollard ρ, the random square algorithms and so on. The security base of Elgamal and ECC (elliptic curves cryptography) is the discrete logarithm problem; current effective discrete logarithm solutions include Shanks, Pollard ρ and Pohlig-Hellman; they may crack Elgamal and ECC cryptography [4].

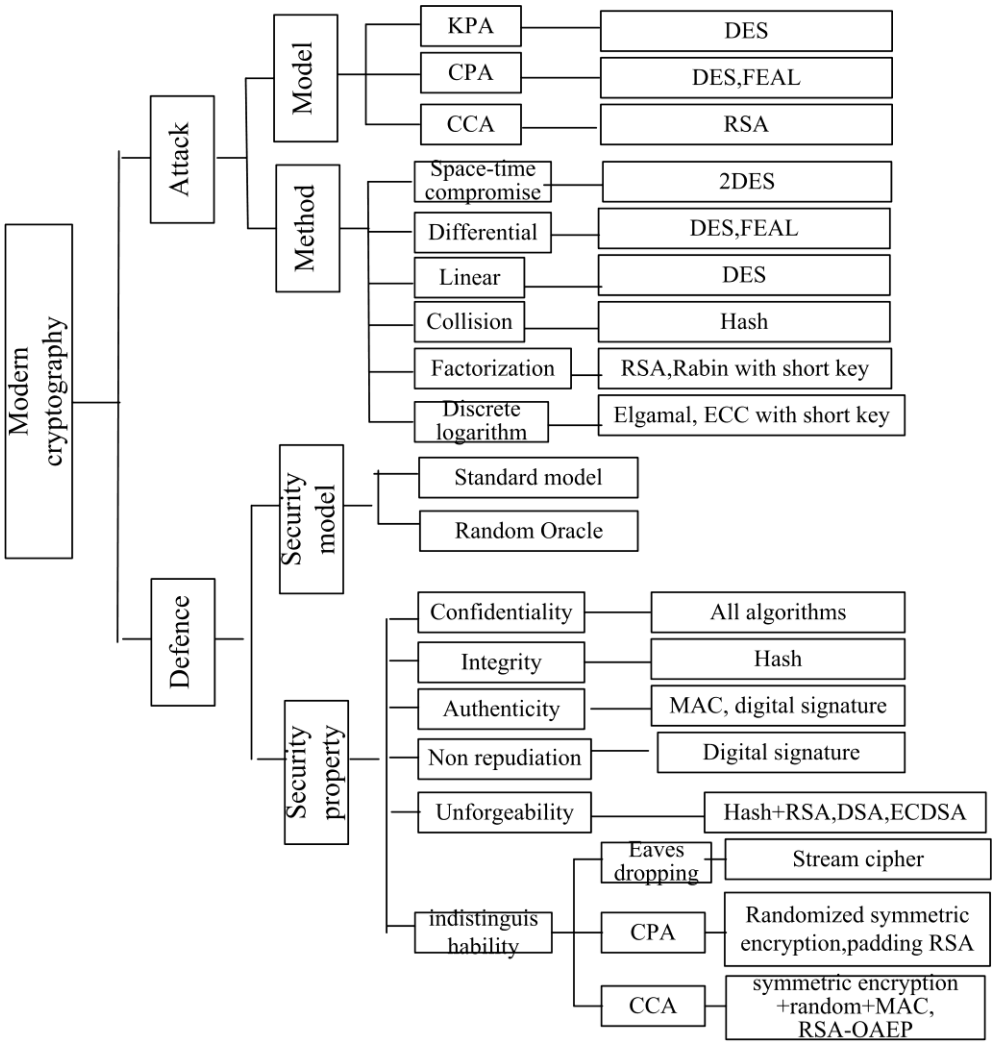


Fig.3. Attack and defense framework of modern cryptography

To resist the threats of eavesdropping, tampering, masquerading and other threats from the Internet, confidentiality, integrity, authenticity and non repudiation are required. Confidentiality is the basic security property of cryptography. Integrity ensures that tampered messages can be detected. To ensure authenticity of the message source, the message authentication code (MAC) is provided. Non repudiation is to solve the conflict problem of communication sides, which is usually achieved by digital signature.

In the provable security theory, a standard model and a random oracle (RO) model are two main models. In the standard model, the security of the algorithm, which needs to be proved, is generally reduced to a standard cryptographic assumption. The RO model has random outputs; the cryptography algorithm with RO is generally efficient. Due to different attack models, indistinguishability is divided into eavesdropping indistinguishability, CPA indistinguishability and CCA indistinguishability. The stream cipher has eavesdropping indistinguishability. Symmetric encryption with a random string has CPA indistinguishability; further combined with MAC, it has CCA indistinguishability. RSA, combined with a random string and RO, has CPA indistinguishability; RSA-OAEP has CCA indistinguishability. Existential unforgeability is security property of digital signature; DSA, ECDSA and RSA with hash are existential unforgeability.

B. Practice Cases in Modern Cryptography. For block ciphers, the encryption and decryption of DES and AES are implemented; then, launch the differential attack and linear attack on the low round DES. For hash functions, MD5 and SHA algorithm are realized; search for a collision through gradual modifications of a message [5, 6]. For public key cryptography, encryption and decryption of

RSA, Rabin, Elgamal and ECC are realized; signature and verification of RSA, DSA and ECDSA are also realized. Under KPA and CPA, RSA has been attacked; the related scenarios are simulated.

For possible attacks on RSA, Rabin and Elgamal ciphers, Fig.4 demonstrates Pollard p-1, Pollard ρ, Shanks, and Pohlig-Hellman algorithms, which are used to solve factorization and discrete logarithm problem.

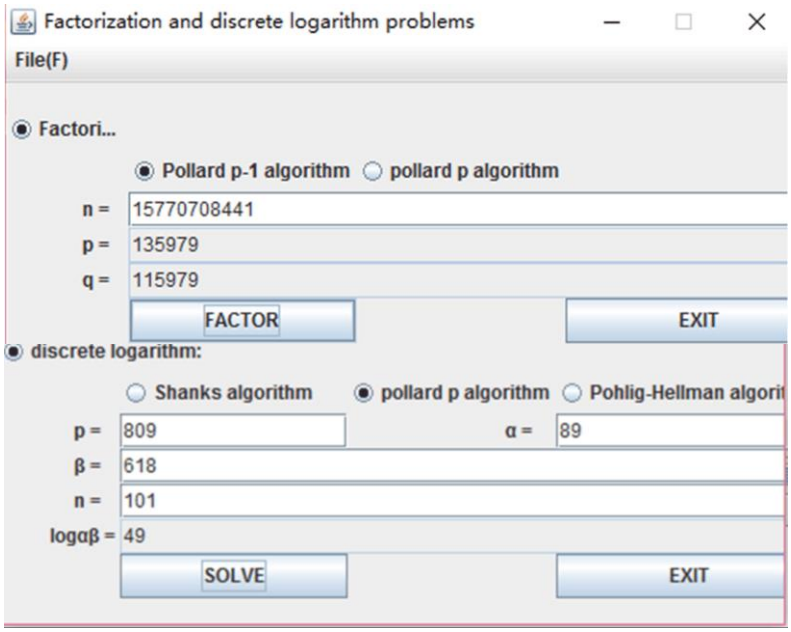


Fig.4. Solution to the factorization and discrete logarithm problems

Conclusions

Attacks and defenses are the focuses of information security. When some new attacks appear, the corresponding defense methods will be proposed. Only the attack means are well understand, defenses are well done. In the paper, attack and defense frameworks in classic and modern cryptography are discussed. Furthermore, the related implementation cases are given. They will provide a reference for enhancing the security of cryptography algorithems.

Acknowledgements

This work was financially supported by the Natural Science Foundation of Anhui Province (1608085MF141), Key Teaching and Research Project of Anhui Province (2013zdjy008) and Quality Engineering Project of Anhui Province (2014zjjh002).

References

[1] Katz J, Lindell Y. Introduction to Modern Cryptography[M]. CRC press, 2014 :50-66.

[2] Stinson D R. Cryptography: Theory and Practice[M]. CRC press, 2005:21-235

[3] Brown D R. Breaking RSA May Be As Difficult As Factoring[J]. Journal of Cryptology, 2016, 29(1):220-241.

[4] Bos J W, Costello C, Hisil H, et al. Fast Cryptography in Genus 2[J]. Journal of Cryptology, 2016, 29(1):28-60.

[5] Andreeva E, Bouillaguet C, Dunkelman O, et al. New Second-Preimage Attacks on Hash Functions[J]. Journal of Cryptology, 2016, 29(4):1-40.

[6] Biham E, Chen R, Joux A. Cryptanalysis of SHA-0 and Reduced SHA-1[J]. Journal of Cryptology, 2015, 28(1):110-160.