Cryptography FAQ (03/10: Basic Cryptology)

Message-ID: <cryptography-faq/part03_1040202968@rtfm.mit.edu>
Supersedes: <cryptography-faq/part03_1038303482@rtfm.mit.edu>
Expires: 22 Jan 2003 09:16:08 GMT
References: <cryptography-faq/part01_1040202968@rtfm.mit.edu>
X-Last-Updated: 1994/07/05
Newsgroups:
sci.crypt,talk.politics.crypto,sci.answers,news.answers,talk.answers
Subject: Cryptography FAQ (03/10: Basic Cryptology)
Followup-To: poster
From: crypt-comments@math.ncsu.edu
Organization: The Crypt Cabal
Reply-To: crypt-comments@math.ncsu.edu
Date: 18 Dec 2002 09:16:16 GMT
X-Trace: 1040202976 senator-bedfellow.mit.edu 3959 18.181.0.29

Archive-name: cryptography-faq/part03
Last-modified: 93/10/10

This is the third of ten parts of the sci.crypt FAQ. The parts are mostly independent, but you should read the first part before the rest. We don't have the time to send out missing parts by mail, so don't ask. Notes such as ``[KAH67]'' refer to the reference list in the last part.

The sections of this FAQ are available via anonymous FTP to rtfm.mit.edu
as /pub/usenet/news.answers/cryptography-faq/part[xx]. The Cryptography FAQ is posted to the newsgroups sci.crypt, talk.politics.crypto, sci.answers, and news.answers every 21 days.

Contents:

3.1. What is cryptology? Cryptography? Plaintext? Ciphertext? Encryption? Key?

The story begins: When Julius Caesar sent messages to his trusted acquaintances, he didn't trust the messengers. So he replaced every A by a D, every B by a E, and so on through the alphabet. Only someone who knew the ``shift by 3'' rule could decipher his messages.

A cryptosystem or cipher system is a method of disguising messages so that only certain people can see through the disguise. Cryptography is the art of creating and using cryptosystems. Cryptanalysis is the art of breaking cryptosystems---seeing through the disguise even when you're not supposed to be able to. Cryptology is the study of both cryptography and cryptanalysis.

The original message is called a plaintext. The disguised message is called a ciphertext. Encryption means any procedure to convert plaintext into ciphertext. Decryption means any procedure to convert ciphertext into plaintext.

A cryptosystem is usually a whole collection of algorithms. The algorithms are labelled; the labels are called keys. For instance, Caesar probably used ``shift by n'' encryption for several different values of n. It's natural to say that n is the key here.

The people who are supposed to be able to see through the disguise are called recipients. Other people are enemies, opponents, interlopers, eavesdroppers, or third parties.

3.2. What references can I start with to learn cryptology?

For an introduction to technical matter, the survey articles given in part 10 are the best place to begin as they are, in general, concise, authored by competent people, and well written. However, these articles are mostly concerned with cryptology as it has developed in the last 50 years or so, and are more abstract and mathematical than historical. The Codebreakers by Kahn [KAH67] is encyclopedic in its history and technical detail of cryptology up to the mid-60's.

Introductory cryptanalysis can be learned from Gaines [GAI44] or Sinkov [SIN66]. This is recommended especially for people who want to devise their own encryption algorithms since it is a common mistake to try to make a system before knowing how to break one.

The selection of an algorithm for the DES drew the attention of many public researchers to problems in cryptology. Consequently several textbooks and books to serve as texts have appeared. The book of Denning [DEN82] gives a good introduction to a broad range of security including encryption algorithms, database security, access control, and formal models of security. Similar comments apply to the books of Price & Davies [PRI84] and Pfleeger [PFL89].

The books of Konheim [KON81] and Meyer & Matyas [MEY82] are quite technical books. Both Konheim and Meyer were directly involved in the development of DES, and both books give a thorough analysis of DES. Konheim's book is quite mathematical, with detailed analyses of many classical cryptosystems. Meyer and Matyas concentrate on modern cryptographic methods, especially pertaining to key management and the integration of security facilities into computer systems and networks. For more recent documentation on related areas, try G. Simmons in [SIM91].

The books of Rueppel [RUE86] and Koblitz [KOB89] concentrate on the application of number theory and algebra to cryptography.

3.3. How does one go about cryptanalysis?

Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. The best available textbooks on the subject are the Military Cryptanalytics series [FRIE1]. It is clear that proficiency in cryptanalysis is, for the most part, gained through the attempted solution of given systems. Such experience is considered so valuable that some of the cryptanalyses performed during WWII by the Allies are still classified.

Modern public-key cryptanalysis may consist of factoring an integer, or taking a discrete logarithm. These are not the traditional fare of the cryptanalyst. Computational number theorists are some of the most successful cryptanalysts against public key systems.

3.4. What is a brute-force search and what is its cryptographic relevance?

In a nutshell: If f(x) = y and you know y and can compute f, you can find x by trying every possible x. That's brute-force search.

Example: Say a cryptanalyst has found a plaintext and a corresponding ciphertext, but doesn't know the key. He can simply try encrypting the plaintext using each possible key, until the ciphertext matches---or decrypting the ciphertext to match the plaintext, whichever is faster.
Every well-designed cryptosystem has such a large key space that this brute-force search is impractical.

Advances in technology sometimes change what is considered practical. For example, DES, which has been in use for over 10 years now, has 2^56, or about 10^17, possible keys. A computation with this many operations was certainly unlikely for most users in the mid-70's. The situation is very different today given the dramatic decrease in cost per processor operation. Massively parallel machines threaten the security of DES against brute force search. Some scenarios are described by Garron and Outerbridge [GAR91].

One phase of a more sophisticated cryptanalysis may involve a brute-force search of some manageably small space of possibilities.

3.5. What are some properties satisfied by every strong cryptosystem?

The security of a strong system resides with the secrecy of the key rather than with the supposed secrecy of the algorithm.

A strong cryptosystem has a large keyspace, as mentioned above. It has a reasonably large unicity distance; see question 8.8.

A strong cryptosystem will certainly produce ciphertext which appears random to all standard statistical tests (see, for example, [CAE90]).

A strong cryptosystem will resist all known previous attacks. A system which has never been subjected to scrutiny is suspect.

If a system passes all the tests mentioned above, is it necessarily strong? Certainly not. Many weak cryptosystems looked good at first. However, sometimes it is possible to show that a cryptosystem is strong by mathematical proof. ``If Joe can break this system, then he can also solve the well-known difficult problem of factoring integers.'' See part 6. Failing that, it's a crap shoot.

3.6. If a cryptosystem is theoretically unbreakable, then is it guaranteed analysis-proof in practice?

Cryptanalytic methods include what is known as ``practical cryptanalysis'': the enemy doesn't have to just stare at your ciphertext until he figures out the plaintext. For instance, he might assume ``cribs''---stretches of probable plaintext. If the crib is correct then he might be able to deduce the key and then decipher the rest of the message. Or he might exploit ``isologs''---the same plaintext enciphered in several cryptosystems or several keys. Thus he might obtain solutions even when cryptanalytic theory says he doesn't have a chance.

Sometimes, cryptosystems malfunction or are misused. The one-time pad, for example, loses all security if it is used more than once! Even chosen-plaintext attacks, where the enemy somehow feeds plaintext into the encryptor until he can deduce the key, have been employed. See [KAH67].

3.7. Why are many people still using cryptosystems that are relatively easy to break?

Some don't know any better. Often amateurs think they can design secure systems, and are not aware of what an expert cryptanalyst could do. And sometimes there is insufficient motivation for anybody to invest the work needed to crack a system.

3.8. What are the basic types of cryptanalytic `attacks'?

A standard cryptanalytic attack is to know some plaintext matching a given piece of ciphertext and try to determine the key which maps one to the other. This plaintext can be known because it is standard (a standard greeting, a known header or trailer, ...) or because it is guessed. If text is guessed to be in a message, its position is probably not known, but a message is usually short enough that the cryptanalyst can assume the known plaintext is in each possible position and do attacks for each case in parallel. In this case, the known plaintext can be something so common that it is almost guaranteed to be in a message.

A strong encryption algorithm will be unbreakable not only under known plaintext (assuming the enemy knows all the plaintext for a given ciphertext) but also under "adaptive chosen plaintext" -- an attack making life much easier for the cryptanalyst. In this attack, the enemy gets to choose what plaintext to use and gets to do this over and over, choosing the plaintext for round N+1 only after analyzing the result of round N.

For example, as far as we know, DES is reasonably strong even under an adaptive chosen plaintext attack (the attack Biham and Shamir used). Of course, we do not have access to the secrets of government cryptanalytic services. Still, it is the working assumption that DES is reasonably strong under known plaintext and triple-DES is very strong under all attacks.

To summarize, the basic types of cryptanalytic attacks in order of difficulty for the attacker, hardest first, are:

cyphertext only: the attacker has only the encoded message from which to determine the plaintext, with no knowledge whatsoever of the latter.

A cyphertext only attack is usually presumed to be possible, and a code's resistance to it is considered the basis of its cryptographic security.

known plaintext: the attacker has the plaintext and corresponding cyphertext of an arbitrary message not of his choosing. The particular message of the sender's is said to be `compromised'.

In some systems, one known cyphertext-plaintext pair will compromise the overall system, both prior and subsequent transmissions, and resistance to this is characteristic of a secure code.

Under the following attacks, the attacker has the far less likely or plausible ability to `trick' the sender into encrypting or decrypting arbitrary plaintexts or cyphertexts. Codes that resist these attacks are considered to have the utmost security.

chosen plaintext: the attacker has the capability to find the cyphertext corresponding to an arbitrary plaintext message of his choosing.

chosen cyphertext: the attacker can choose arbitrary cyphertext and find the corresponding decrypted plaintext. This attack can show in public key systems, where it may reveal the private key.

adaptive chosen plaintext: the attacker can determine the cyphertext of chosen plaintexts in an interactive or iterative process based on previous results. This is the general name for a method of attacking product ciphers called `differential cryptanalysis'.

The next part of the FAQ gives the mathematical detail behind the various types of cryptoanalytic attacks.

Part01 - Part02 - Part03 - Part04 - Part05 - Part06 - Part07 - Part08 - Part09 - Part10

[By Archive-name | By Author | By Category | By Newsgroup]
[Home | Latest Updates | Archive Stats | Search | Usenet References | Help]

Send corrections/additions to the FAQ Maintainer:
crypt-comments@math.ncsu.edu

Last Update January 01 2003 @ 00:33 AM