2 17 24 15 19 14 6 17 0 15 7 24

Sarah Busch and Lorna Karaj

Final Project for MA 341

Appreciation of Number Theory

Boston University Summer Term 2009

Instructor: Kalin Kostadinov

Cryptography is an ancient art, which has become an important tool in today's superfluous use of un-trusted, communication mediums. Cryptography comes from the Greek words cryptos, hidden, and logia, write, and is the study of secret information. Its first use can be dated back to 1900 B.C.E. when an Egyptian scribe used a non-standard form of hieroglyphics. It can be argued that cryptography developed immediately after the invention of writing in order to conceal war plans. Today cryptography is particularly important when communicating over the Internet and sharing personal data.

There are many uses for cryptography. Firstly, it ensures confidentiality and protection of one's identity. Secondly, cryptography is used to maintain the integrity of certain data and to prevent data alteration. Thirdly, authentication ensures the data is not false and does not originate from a different party.

The four cryptographic primitives include: secret-key encryption, public-key encryption, cryptographic signing, and hash functions. Secret-key encryption, or symmetric cryptography, transforms the data to be unreadable by anyone who does not own the secret key, which encrypts and decrypts the data. Secret key-algorithms are called block ciphers (like RC@, DES, TripleDES and Rijndael) and are used to interpret one block at a time. The ciphers transform an input block of n bytes into an output block. But because n is small, any encryption bigger than n has to be encrypted one block at a time. Block cipher classes use a chaining mode called cipher block chaining (CBC) which uses a key and a vector (IV) to change the data. Without the IV someone can decipher the message but if the initial vector is used to create the first block, then the first block can be used to create the second block and so on. This prevents users from using common message headers to reverse engineer the key. This data can be compromised by searching for every possible key, but doing so would be incredibly time consuming and impractical.

Public-key encryption, or asymmetric cryptography, transforms the data to prevent its legibility by a third party. This uses a public and a private key to encrypt and decrypt the data. This encryption contains a public key that can be made public to anyone and a private one that is kept a secret. The keys are mathematically linked in such a way that the data encrypted with the public key can only be decrypted with the private key and the data signed with the private key can only be authenticated with the public key.

Unlike the symmetric encryption, here one key is used to encrypt and one to decrypt, so two keys are required to interpret the data. The public key algorithm uses a fixed buffer size while the secret key uses a variable-length buffer. The public key also has a larger keyspace and a bigger range of possible values so it would be even more inefficient to try to figure out the key by exhausting every possibility.

Cryptographic signing verifies that the data comes from a specific party by creating a digital signature that pertains to that party. Public keys can be used to also create signatures, which verify the identity of the user. But this identity is identifiable by the public because the sender's public key is included in the signature format.

Cryptographic hashes transform data of any length to fix a fixed byte sequence, which is unique. Hash algorithms change arbitrary length values to fixed length values known as hash values. Hash values are unique and it is unusual to find two inputs that hash the same way. There are two types of hash functions: Message authentication code (MAC), which is used for digital signatures and message detection code (MDC), which is used for data integrity.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

http://www.garykessler.net/library/crypto.html

RSA is the current algorithm for public key cryptography and it is used for encryption as well as signing. The RSA algorithm was made public in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman and it includes key generation, encryption and decryption. In key generation the RSA has a public and a private key, which a user can get by choosing two distinct prime numbers p and q. We compute $n= pq$ where n is the modulus for the public and private key. Then we compute the quotient $\varphi(n) = (p - 1)(q - 1)$. Then we choose an integer e such that $1 < e < \varphi(n)$ and e and $\varphi(n)$ are relatively prime. e is the public key component. Finally we determine d such that $de \equiv 1(\text{mod } \varphi(n))$ where d is the private key exponent. In encryption the public key (n, e) is transmitted. The message M is turned into an integer $< m < n$ by using a reversible protocol known as padding scheme. Then c is transmitted such that $c \equiv m^e$ (mod n). Finally in decryption using the private key exponent d, we can use $m \equiv c^d$ (mod n) to recover the original message.

To illustrate all of this we can take a simple example that shows the use of the RSA algorithm in practice:

If we take p=23 and q=11, we get n=253.
Then $\varphi(253)=22*10 =220$
We take e coprime to 220 where $1 < e < 220$. If e=13…
We find d where d≡1(mod 220) so d =17.
n= 253 and e = 13 are made public so that E is easy to find.

If the message sent is “YEAH” and we know n and e, the message is written as

25 5 1 8

The person sending it computes:

$E(25) = 25^e = 25^{13} = 27$
$E(5) = 15^e = 15^{13} = 13$
$E(1) = 1^e = 1^{13} = 1$
$E(8) = 8^e = 8^{13} = 248$

And sends the following encrypted message:

27 136 1 248

When received each number has to be raised to d in order to be decrypted:

$27^{17} = 25$

$136^{17} = 5$

$1^{17} = 1$

$248^{17} = 8$

Which translates into the previous message: “YEAH”

Another example of the use of cryptography is in ensuring fairness during an out of sight decision by using public key-algorithm. As noted before, an advantage of the asymmetric encryption is that the two people sending the message (hypothetically called as Mary and Tom) never need to meet to exchange keys such as would be required for the symmetric encryption. An example would be when Mary and Tom want to go see a movie, but they cannot agree on which one. So they decide to flip a coin over it. The problem is that they are doing this over the phone, so either of them could cheat. Using public key algorithm, they can both make sure that there is fairness in the coin flip. When Mary flips her coin, she sends that message to Tom via a public key, which can only be decrypted by Tom with his private key. Tom does the same and when the message is sent back they both have to use their own private key and the other person’s public key in order to decrypt the message they received, thus ensuring fairness.

Encryption and decryption is most used in times of war when secrecy is crucial to a country’s success in the element of surprise and attack. It was extensively used during World War II with the decoding of the Zimmermann telegram and the most successful one being the decryption of the German “Enigma” Cipher in 1932 by Poland and then passed on to France and Britain by 1939. The decryption proved to be essential throughout the war. It allowed the Allies to read parts of German radio traffic. Such military intelligence came to be called Ultra. Another example of cryptography’s application is that of the Japanese cipher (PURPLE), which allowed entrance into the highest diplomatic Japanese security before the United States even entered the war.

Cryptography was also used during the Cold War when the United States first started using the wire trapping industry, which Russia used on site agents. The U.S. created the National Security Agency and the Echelon network, which listens to all electronic communications, including telephones and computers. Then the messages are filtered to produce trigger alerts when something of “interest” comes up. There came a time, where national security became so important that in some countries obscure agencies put restrictions on research projects that included data integrity algorithms and forbade scientific publications of that kind.

Today the situation is much more liberal and cryptography is not only used but studied and taught. Size is very important in modern cryptography especially because of computers. The larger the key is, the harder it is to try to crack the code forcefully. Surprisingly secrecy is not the most important aspect to cryptographic algorithms. The best algorithms are those well studied and documented because they are well tested.

Sources

http://msdn.microsoft.com/en-us/library/92f9ye3s(vs.71).aspx
http://en.wikipedia.org/wiki/RSA
http://en.wikipedia.org/wiki/World_War_II_cryptography
http://www.garykessler.net/library/crypto.html
http://books.google.com/books?id=DVLEql738mwC&pg=PA13&lpg=PA13&dq=cryptography+during+the+cold+war&source=bl&ots=IljpL1zFtq&sig=u3gArf01l9zfaCUcsFiUqcH7544&hl=en&ei=GgY4Sr_6Lo2-lAeR4-zuDQ&sa=X&oi=book_result&ct=result&resnum=7#PPA13,M1
http://www.andreasholmstrom.org/teaching/sma205/lecturenotes/sma205pages59to65.pdf