MODERN CRYPTOGRAPHY
FOR
INFORMATION SECURITY
APPING2: [Level I]

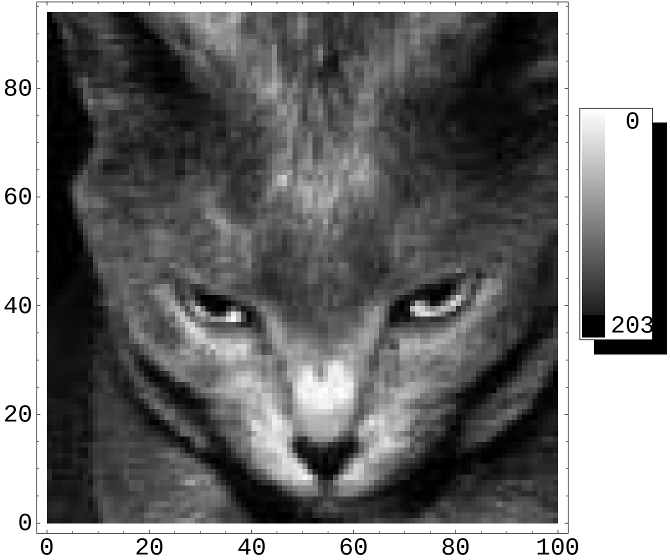
cryptoing2@gmail.com

Introduction

Modern Cryptography for IS

1. Pictures
2. A short scenario
3. The TLS/SSL protocol
4. Objectives of the course
5. An enigma
6. Some Information Security objectives
7. Some Fundamental Cryptographic goals
8. Asymmetric and symmetric cryptography
9. Digital Signature
10. Authentication and identification
11. The Bernstein Case

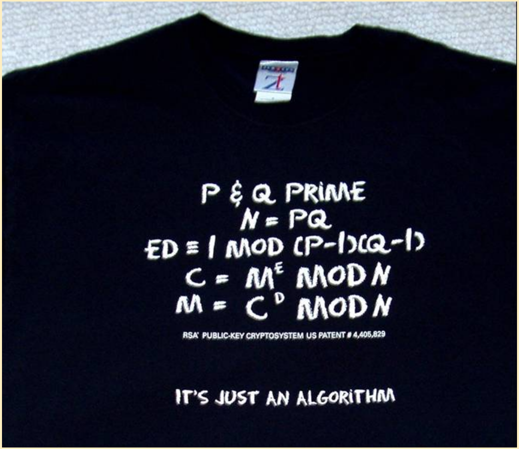
A picture we will use sometimes



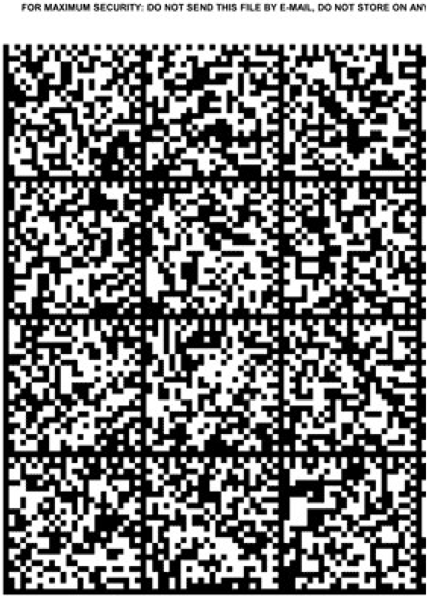
A nice picture

WARNING
This shirt is classified as a munition
and may not be exported from the United States,
or shown to a foreign national
RSA
encryption in perl
etty Good Priva

September 17th 2000 : 1000 gifts from *RSA Data Securiy*!



A RSA key of 2048 bits in a flashcode



FOR MAXIMUM SECURITY: DO NOT SEND THIS FILE BY E-MAIL, DO NOT STORE ON ANY

Where can we find/use cryptography ?

- Password : Unix and Windows
- Smartcards
- X509 Certificate
- SSL/TLS
- IPsec/IPv6
- HTTPS :// HTTP Secure (this is a little bit exagerated)
- KERBEROS : Authentication service
- Malware : unfortunately for Malware Analysts
- Cryptocurrencies : blockchain, signature with Elliptic Curves
- S/MIME
- etc.

You want to buy a book (or anything else) on Internet ?

Ok, this means :

1. You have to run your favorite internet browser
2. You have to go to your favorite site : http ://www.internetbookseller.com
3. You have to choose your book *How I have learned Cryptography*
4. You have to « click » on something like « Sell now »
5. And you suddenly switch on another website https ://www.internetbookseller.com
6. And then : you have to pay !

Do you read now https ://www.internetbookseller.com ?

Yes, and this means (generally) :

1. The web site sent to your internet browser :
   1. something like a public key (an RSA couple (n, e) for example)
   2. or a Diffie-Helmann key (p, g) with an ephemeral key $g^b \bmod p$
2. Your internet browser sent an answer
3. And all other communications will be ciphered or encrypted with a symmetric cipher algorithm

HTTPS ? (wikipedia/IETF)

1. HTTPS : also called HTTP over TLS, HTTP over SSL, and HTTP Secure
2. It is a protocol for secure communication over a computer network (widely used on the Internet).
3. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer (SSL).
4. Main motivation for HTTPS is *authentication* (of the website) and to protect the *privacy* and *integrity* of all exchanged data.

HTTPS ? (wikipedia/IETF)

This means : you have to make choices : algorithms and keys. We will review the main algorithms you can use.

1. You are the Client ?
   - Then you have to chose algorithms you accept to use
   - You have to compute keys : secret and public
   - In the real world : You do nothing, you just use it (see Transparency)
2. You are the Server ?
   - Then you have also to chose algorithms you accept to use
   - And you have also to compute keys : secret and public
   - In the real world : You sometimes do something, you can just use it.

TLS (cf IETF)

1. SSL : Secure Socket Layer
2. SSL : Originally developed by Netscape
3. Netscape's patent buyed in 2001 by l'IETF
4. Now called TLS : *Transport Layer Security*
5. TLS is a client-server model
6. Request For Comments (RFC/IETF) : RFC 4346 + RFC 5246 + RFC 6101

Transport Secure Layer : objectives

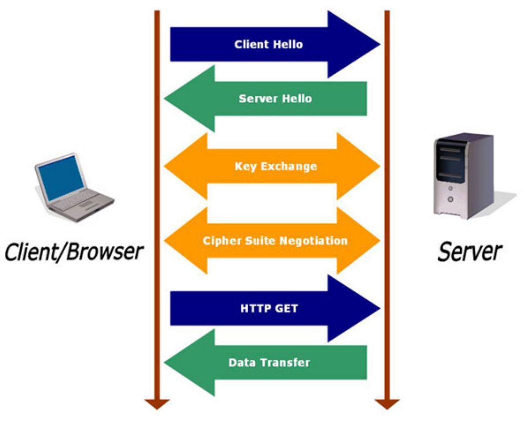
1. Authentication : Who is on the other side ?
   - Server Authentication — required [*via* PKC and possibly with a X.509 certificate]
   - Client authentication — optional
2. Confidentiality of all data exhanged : *via* symmetric cryptography
3. Integrity : messages integrity *via* hash functions
4. Spontaneity : any Client contacts Server (possibly for the first time) without problem
5. Transparency : You do not want to know about security, so you do not have to modify http, you just use it.

SSL (cf RFC 6101) : The SSL protocol provides connection . . .

. . . security that has three basic properties :

1. The connection is **private**. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g., DES [*dead/obsolete*], 3DES , AES, FORTEZZA, RC4).
2. The peer's identity can be **authenticated** using asymmetric, or public key, cryptography (e.g., RSA , DSS).
3. The connection is **reliable**. Message transport includes a message integrity check using a keyed Message Authentication Code (MAC) [RFC2104]. Secure hash functions (e.g., SHA, MD5) are used for MAC computations.

Image ! (cf ssl.trustwave.com)



Modern Cryptography for IS

Contents :

1. Symmetric cryptography algorithms : DES/3DES/3DES + AES
2. Mathematical prerequisites : groups, rings, fields, how to compute a prime number ? Elliptic curves, etc.
3. Asymmetric cryptography algorithms : RSA, DH
4. Hash functions : MD4/MD5/SHA1/SHA3
5. Protocols : TLS/SSL + SSH (if we have time)
6. A little bit of RSA cryptanalysis (if we have time)
7. An exam (short : 1h30 or 2h)

An enigma from [?] :

« Alice wants to send a gift to Bob. She does not trust the escort ship. She knows that if she uses a locked trunk (at least one), the escort ship will do the job. What can she do ? »

A game about the enigma :

Just play the following « game » :

1. Think to some different protocols
2. For each of them : find a weakness (a flaw) and try to fix it.

Protocol with four travels (non cryptographic)

1. Alice sends the trunk : locked with K_{Alice} (private)
2. Bob sends the trunk : locked now with K_{Bob} and K_{Alice} (private unknown from Alice), two padlocks.
3. Alice receives the locked trunk, unlock it with her key K_{Alice}.
4. Alice sends the locked trunk : locked it with Bobs key : K_{Bob}.
5. Bob receives the locked trunk, unlock it with the Alice's key : K_{Alice}.

Interest

1. Alice can sent a gift without knowing Bob

Weaknesses

1. Bob does not know who has really sent the trunk
2. Bob can say to Alice : I've received nothing from you
3. Non cryptographic (today but in the future ?)

Symetric Protocol (with less travels, cryptographic) :

1. Alice and Bob decides a common « key » (in a set of keys) (secret, known from Alice and Bob) with a secure channel.
2. Alice sends the locked trunk : locked with their common key $K_{Alice+Bob}$.
3. Bob receives the locked trunk, unlock their key .

Interest

1. Cryptographic

Weaknesses

1. Again, if Alice can not discuss with Bob, she can do nothing
2. Bob does not know who has sent the trunk but Alice can put a message into the trunck
3. Bob can say to Alice : I've received nothing from you

Symetric Protocol :

1. Alice sends the locked trunk : locked with her key K_{Alice} (secret, known from Alice).
2. Bob receives the locked trunk, he waits.
3. Alice sends the key to Bob, with or without a trusted escort ship.
4. Bob unlock the padlock.

Interest

1. Bob can receive a gift without knowing Alice
2. Cryptographic (PGP)

Weaknesses

1. What if the escort ship (not trusted) keeps the « true » trunk and gives another trunk to Bob ?
2. Bob can say to Alice : I've received nothing from you

An asymmetric protocol :

1. Bob publishes the « number » of his public padlock
2. Alice buys the Bob's public padlock
3. Alice sends the locked trunk : locked with Bob's public padlock
4. Bob receives the locked trunk, unlock with his key K_{Bob} (private, unknown from Alice).

Interest

1. Anyone can sent to Bob a gift

Weaknesses

1. How can Bob be sure it's really Alice's gift ?
2. How can Alice be sure that she has spoken with Bob ?
3. Bob can say to Alice : I've received nothing from you
4. Alice can say to Bob : hum, I've sent nothing to you

Some Information Security (IS) objectives ([?])

1. Confidentiality (or Privacy) : to keep information secret from all but those who are authorized to see it.
2. Data Integrity : to ensure information has not been altered by unauthorized or unknown means.
3. Entity Authentication (or identification) : corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.).
4. Message Authentication : to corroborate the source of information ; also known as data origin authentication.
5. Signature : a means to bind information to an entity.

Some other objectives of IS

1. Authorization conveyance : to another entity, of official sanction to do or be something.
2. Validation : a means to provide timeliness of authorization to use or manipulate information or resources.
3. Access control : to restrict access to resources to privileged entities. certification endorsement of information by a trusted entity.
4. Timestamping : to record the time of creation or existence of information. witnessing verifying the creation or existence of information by an entity other than the creator.

Some other objectives of IS

1. Receipt : acknowledgement that information has been received.
2. Confirmation : acknowledgement that services have been provided.
3. Ownership : a means to provide an entity with the legal right to use or transfer a resource to others.
4. Anonymity : to conceal the identity of an entity involved in some process.
5. Non-repudiation : to prevent the denial of previous commitments or actions.
6. Revocation : retraction of certification or authorization.

Some Fundamental Cryptographic goals

1. Confidentiality is a service used to keep the content of information from all but those authorized to have it. Secrecy is a term synonymous with confidentiality and privacy. There are numerous approaches to providing confidentiality, ranging from physical protection to mathematical algorithms which render data unintelligible.
2. Data integrity is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

Some Fundamental Cryptographic goals

1. Authentication is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes : entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).
2. Non-repudiation is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.

Kerckhoffs' principal is a set of requirements for cipher systems . . .

. . . given here essentially as Kerckhoffs originally stated them :

1. The system should be, if not theoretically unbreakable, unbreakable in practice.
2. Compromise of the system details should not inconvenience the correspondents.
3. The key should be rememberable without notes and easily changed.
4. The cryptogram should be transmissible by telegraph.
5. The encryption apparatus should be portable and operable by a single person.
6. The system should be easy, requiring neither the knowledge of a long list of rules nor mental strain.

This list of requirements was articulated in 1883 and, for the most part, remains useful today. Point 2 allows that the class of encryption transformations being used be publicly known and that the security of the system should reside only in the key chosen.

Asymmetric cryptography/ Public-key cryptography [?, ?, ?]

Public-key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys, a public key and a private key :

- The private key is kept secret,
- The public key can be widely distributed or published.

The keys are (generally) related mathematically, but the private key cannot be practically computed from the public key. We say that the problem of finding the private key from the public key is *computationally difficult*.
A message encrypted with the public key can be decrypted (generally) only with the corresponding private key.
Conversely, secret key cryptography, also known as symmetric cryptography uses a single secret key for both encryption and decryption. Bith the ender and the receiver know the secret key.

The two main branches of public key cryptography are :

- Public key encryption : a message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. This is used to ensure confidentiality. (Well : we suppose it's computationally difficult.)
- Digital signatures : a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This is used to ensure authenticity. (Well : we suppose that forging a « true fake » signature is computationally difficult.)

PKC : Algorithms ?

- RSA := Rivest - Shamir - Adleman : Cipher + Signature+ Key agreement protocols + Transport Key Protocols
- El Gamal : Cipher + Signature
- DH :=Diffie-Hellman : Key agreement protocols + Transport Key Protocols
- Elliptic curves : Cipher + Signature + Key agreement protocols + Transport Key Protocols
- etc.

Modern Cryptography for IS

Symmetric cryptography :

- Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.
- The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and to their applications. A block cipher is, in a sense, a modern embodiment of Vigenere's or Alberti's polyalphabetic cipher : block ciphers take as input a block of plaintext and a key, and output a block of ciphertext of the same size. Since messages are almost always longer than a single block, some method of knitting together successive blocks is required. Several have been developed, some with better security in one aspect or another than others. They are the mode of operations and must be carefully considered when using a block cipher in a cryptosystem.

Symmetric Algorithms ?

- nDES : Data Encryption Standard (block cipher) : obsolete !
  1. DES : block cipher, $|K| = 56$ bits, *dead*
  2. double-DES (2DES) block cipher, $|K| = 112$ bits, *obsolete*
  3. Triple DES (3DES) : block cipher, $|K| = 168$ bits, *alive*
- AES : Advanced Encryption Standard : block cipher, $|K| = 128$ or $|K| = 186$ or $|K| = 256$ bits, *alive*
- FORTEZZA : *NSA cryptography, deprecated*, **[?]** :"*Fortezza Crypto Card, a PC Card-based security token. It was developed for the U.S. government's Clipper chip project and has been used by the U.S. Government in various applications.*"
- RC4 : Ron's Cipher (stream cipher), *quite dead*
- etc.

How to use (securely) an algorithm ?

1. How to create/choose/compute a key ?
2. How to cipher ?
3. How to decipher ?
4. How to Sign (for asymetric algorithms) ?
5. How to choose/create « secured » keys (mainly for asymetric algorithms) ?
6. How to secure the whole stack : algorithm, codes, keys ?

Digital Signature

A cryptographic primitive which is fundamental in authentication, authorization, and nonrepudiation is the digital signature. The purpose of a digital signature is to provide a means for an entity (A) to bind its identity to a piece of information. The process of signing entails transforming the message and some secret information held by the entity into a tag called a signature. A generic description follows.

1. M is the set of messages which can be signed.
2. S is a set of elements called signatures, possibly binary strings of a fixed length.
3. S_A is a transformation from the message set M to the signature set S, and is called a signing transformation for entity A. The transformation S_A is kept secret by A, and will be used to create signatures for messages fromM.
4. V_A is a transformation from the set $M \times S$ to the set *{true,false}*. V_A is called a verification transformation for A's signatures, is publicly known, and is used by other entities to verify signatures created by A.

Digital Signature

Signing procedure : the signer entity A creates a signature for a message $m \in M$ by doing the following :

1. Compute $s = S_A(m)$.
2. Transmit the pair (m, s) : s is called the signature for message m.

Verification procedure : To verify that a signature s on a message m was created by A, an entity B (the verifier) performs the following steps :

1. Obtain the verification function V_A of A.
2. Compute $u = V_A(m, s)$.
3. Accept the signature as having been created by A if u =true, and reject the signature if u = false.

Authentication

It's a term which is used (and often abused) in a very broad sense. By itself *authentication* has little meaning other than to convey the idea that some means has been provided to guarantee that entities are who they claim to be, or that information has not been manipulated by unauthorized parties. Authentication is specific to the security objective which one is trying to achieve. Examples of specific objectives include

1. Access control
2. Entity authentication
3. Message authentication
4. Data integrity
5. Non-repudiation
6. Key authentication.

Modern Cryptography for IS

Authentication : If Alice and Bob desire assurance of each other's identity, there are two possibilities to consider :

1. Alice and Bob could be communicating with no appreciable time delay. That is, they are both active in the communication in 'real time'.
2. Alice or Bob could be exchanging messages with some delay. That is, messages might be routed through various networks, stored, and forwarded at some later time.

In the first instance Alice and Bob would want to verify identities in real time. This might be accomplished by Alice sending Bob some challenge, to which Bob is the only entity which can respond correctly. Bob could perform a similar action to identify Alice. This type of authentication is commonly referred to as entity authentication or more simply identification. For the second possibility, it is not convenient to challenge and await response, and moreover the communication path may be only in one direction. Different techniques are now required to authenticate the originator of the message. This form of authentication is called data origin authentication.

Identification

An identification or *entity authentication* technique assures one party (through acquisition of corroborative evidence) of both the identity of a second party involved, and that the second was active at the time the evidence was created or acquired. Typically the data transmitted is only that necessary to identify the communicating parties. The entities are both active in the communication, giving a timeliness guarantee.

Identification : example

1. An instance of mutual authentication (identification) : Alice calls Bob on the telephone. If Alice and Bob know each other then entity authentication is provided through voice recognition. Although not foolproof, this works effectively in practice.
2. Unilateral authentication (identification) : Alice provides to a banking machine a personal identification number (PIN) along with a magnetic stripe card containing information about Alice. The banking machine uses the information on the card and the PIN to verify the identity of the card holder. If verification succeeds, Alice is given access to various services offered by the machine.

http ://textfiles.com/magazines/ICS/ics2-6.txt

ITAR=International Traffic in Arms Regulations [?]

The EFF lawsuit, filed in February of 1995, challenges the ITAR export- control scheme as an "impermissible prior restraint on speech, in violation of the First Amendment." The plaintiff in the suit is Daniel Bernstein, a graduate student in mathematics from UC-Berkeley who has developed a new encryption algorithm and wishes to publish and discuss his work with colleagues and the general public (what would be a violation of the existing regulations). Bernstein is contending that software and its documentation "are published, not manufactured ; they are Constitutionally protected works of human-to-human communication, like a movie, a book, or a telephone conversation".

Remark : EFF=Electronic Frontier Foundation [?]

- Electronic Frontier Foundation (EFF).
  http ://www.eff.org.

- D. Kahn.
  The Code Breakers. The story of secret writings.
  Mac Millan Publishing Company, 1967.
  (réédité en 2000).

- A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone.
  Handbook of Applied Cryptography.
  CRC Press, 1997.
  http ://cacr.uwaterloo.ca/hac/ (all chapters available for free download).

- Press Release.
  Eff sues to overturn cryptography restrictions.
  "http ://www.eff.org/pub/EFF/Policy/Alerts".

- D. Stinson.

Cryptography.
1994.

WIKIPEDIA.
http ://www.wikipedia.org.