EE720 : Introductory Lectures

Virendra Sule
Dept. of EE
IIT Bombay

August 10, 2020

1 Security in Communication

When two parties Alice and Bob are physically at distinct locations and want to communicate they must set up a mechanism for transacting information bits. Sometimes as in the case of one party being a machine, such a mechanism is still required for information transaction even if they are in the same place. Transaction of information is required for data storage, queries, bulk data communication, authentication of messages as well as in tasks such as priority and que ordering, gaming, sharing, digital cash mechanisms etc. Two primary issues that arise in all these situation are, one the mechanism of transaction must be *efficient* in terms of ease of use, cost of infrastructure, time required, energy consumption and second the scheme of transaction must be *secure*. We can identify following primary security concerns:

1. Disruption of transaction functionality, communication quality and services by malicious intention.
2. Unlawful access to communication infrastructure or content.
3. Compromise of privacy of communication of authentic parties either by tracking their locations or eavesdropping to recover content partially or tampering with the information communicated.
4. Impersonation by authentic parties as well as attack on identification of authentic parties.
5. Confidentiality of content (or Information) of communication and integrity of confidential content.

Addressing these security issues and achieving a secure communication system has been still not been perfectly achieved. However what has been achieved in practice to a reasonable extent using cryptography is still very valuable. Goals of cryptography are summarized below. Formally, Cryptography is the science which addresses following issues

1. *Confidentiality* of information. Requirement that Information be accessible only to parties which have been authorized to access the content.

2. *Integrity* of information. Requirement that during communication of information any intentional unlawful tampering of information be detectable. Also amounts to authenticating the correctness of the information content.

3. *Authentication* of identities: Identification of lawful parties who have communicated.

Another security feature sometimes necessary in transaction is *non-repudiation* by which a party cannot disown information authenticated by her/his identity. In a larger sense one can say that the goal of cryptography is to create a (relatively) secure channel for information exchange using an insecure channel itself which is likely to be attacked by intrusion.

In ancient times prior to Ceaser, confidentiality was achieved by secrecy or hiding communication. However secrecy has its own costs and failures are fatal. Cryptography developed in response to minimizing secrecy of communication to achieve confidentiality. But if a confidential communication is not hidden then the content of communication has to be made computationally infeasible for the adversary to read from the encrypted content communicated. Such a notion of security in encryption is called *Computational Security*. Alternatively the encryption is perfectly secret if the a priori information about the content is the same as a posteriori information about the content available from ciphertext. Such a notion of security of encryption is called *Information theoretic* security. These two trends of thought have been principal ways of establishing the notion of security in modern cryptography. However measuring an extent of security of a cryptographic method has evolved simultaneously with cryptographic research and much of cryptography relies heavily on computational security related to unsolved problems. The study of measuring extent of security and exploring weaknesses in encryption methods is called *Cryptanalysis*.

1.1 What is cryptology

Cryptology is the combined term for *Cryptography* and *Cryptanalysis*. We first introduce these basic terms.

- *Cryptography* is the science concerned with encryption of information. A primary goal of cryptography is to achieve *Confidentiality* of information, the information communicated is required to be restricted only to specific entity. Confidentiality can be achieved by encryption of information using a *key* in two different ways. By one the key is shared securely between communicating entities called *symmetric* key encryption. By another the encryption key (called public key) is uniquely tied to a secret decryption key (called private key). This method is called *asymmetric* or *public* key encryption. The public key is required to be securely bound to the identity of the entity. Hence method for sharing the key and binding the public key to the identity are also goals of cryptography. This method solves two problems in one go, that of confidentiality of information and authentication of the entity provided appropriate security conditions hold.

- *Cryptanalysis* is concerned with estimating difficulty of subverting functionality of cryptography. This allows evaluation of cryptographic schemes for their duration of utility and possible upgradation of security. In extreme cases this may be useful for carrying out subversion of confidentiality of adversary's cryptography.

- Coding. Concerned with (optimal) representation of information (data compression or source coding) and correcting errors occurring during transmission of information (channel coding). Coding is not concerned with confidentiality but is meant for accurate communication of information over realistic channels which cause corruption of the information passing through the channel due to inherent noise. Sometimes older literature refers to encrypted information as codes and cryptanalysis as code breaking. However coding is necessary to communicate encrypted information correctly so that it can be decrypted by the authentic entity. Due to this separation between confidentiality and correctness of communication of information, Cryptography in the past has been oblivious of the coding. However the purpose of encryption is primarily to encode information which is decoded by the authentic party. Hence encryption should ideally be *coding aware* especially if confidentiality and authentication is a required on the physical channel of communication where only encoded physical signals can be transmitted.

The discipline of Cryptology encompasses Cryptography and Cryptanalysis. Some of the good texts in cryptography are [6, 3, 5, 8]. Reference [6] is particularly useful to understand functions and importance of cryptography in various practical situations. A voluminous treatise which contains technical discussions of algorithms is [7]. Cryptographic protocols used in communication and their security is discussed in [9]. Several new approaches for public key Cryptography, Cryptography over physical channel and key exchange over physical channel are being discovered and researched. Cryptology is a very vast subject and has strong interactions with computation, computing technologies, mathematics, commerce and currency, social networking and now even politics.

Excercise 1. Consider the task of devising your own scheme for confidentiality of communication between a group of your "friends". If some of your friends have malicious intentions, how will you keep your personal diary and communication confidential, while keeping your actions and communication open for scrutiny. Document all the risks involved in this scheme. Document all procedures you will follow.

1.2 How to achieve confidentiality?

A message to be sent by Alice meant for Bob is securely transmitted if a third party Eve cannot extract the information about the message in the ciphertext. From the point of view of computational security this process requires what is called a *Trapdoor One Way Function* (TOWF). First we define a *One Way Function* (OWF).

Let X be a set of strings over symbols (such as $\{0, 1\}$) and Y another set (possibly of strings) over these symbols. A function $f : X \to Y$ is said to be a OWF if

1. Given a string x in X producing $y = f(x)$ is "Easy".
2. But given y in Y producing x in X such that $y = f(x)$ even with the knowledge that such an x exists is "Difficult".

Here "Easy" and "Difficult" are computationally relative notions. They are meant to be associated with computational efforts. If n is the largest number of bits required to

represent all elements of X (called the length of cardinality of X and is equal to $\log_2 |X|$) then computationally "Easy" means that the effort required in achieving the result (the time and storage space) is of polynomial order in n denoted $O(n^k)$. "Difficult" means that there is no known polynomial time algorithm to solve the problem. A measure of computational complexity is given by the following formula in which the cardinality $|X| = N$ is of exponential order. Hence computational effort is measured in terms of $n = \log_2 N$ the number of bits required to encode objects in the set of cardinality N.

$$L_N(c, \epsilon) = O(\exp[c(\log N)^{\epsilon}(\log \log N)^{1-\epsilon}]$$

which is of *polynomial* order $O((\log N)^c)$ for $\epsilon = 0$ and *exponential* order $O(\exp(c \log N))$ for $\epsilon = 1$. For $0 < \epsilon < 1$ the order of complexity is called *sub-exponential*.

Hence we can consider a function $y = f(x)$ mapping from a set X to Y, to be practically a OWF if we can show that the the "easy" and "difficult" computations above are practically "easy" and "infeasible" respectively, if we dont have a theoretical proofs of bounds of their order of computational time.

Excercise 2. Can you think of mathematical examples of OWFs? Do you know physical OWFs which are transformations of physical signals whose information bits denoted x transform into physical signals with information bits y and X, Y are corresponding spaces of information strings of physical signals?

Excercise 3. Let $N = 2^n$. For $r < N$ let

$$m = f(r) = \begin{pmatrix} N \\ r \end{pmatrix}$$

Is $f(.)$ a relative OWF? what are the relative bounds for computation $y = f(x)$ and inverting x to y.?

Excercise 4. Let S_m denote permutation of m elements. The cardinality $|S_m| = m!$. Let $n < m!$ and let a set $\{P_0, P_1, \ldots, P_{n-1}\}$ be given with P_i in S_m. For $x = (x_0, \ldots, x_n)$ a string of n bits, define

$$y = f(x) = \prod_{x_i=1} P_i$$

This defines a function $f : \{0, 1\}^n \to S_m$. Is f a OWF?

In general constructing OWFs theoretically is an open problem. However you should think of many ways to interpret the forward $y = f(x)$ and reverse computation for a practical OWF. First of all the sets X, Y must have large cardinalities so that just brute force search for x given y should not be feasible. Then to defeat any search which is guided by the structure of f the image y of a random x must be as much uniformly distributed over Y in the sense that f should not show any bias. Another way to interpret the rnadomness of mappin f is that if X and Y are subsets in a finite field, then a random line $ax + by + c = 0$ must have as much close to half probability of satisfying the equation $y = f(x)$. Many such criteria have been constructed. The topic of OWF is a fundamental issue in computational science.

Excercise 5. Consider the function $y = 2^x \mod p$. Where p is an odd prime number. Determine the practical comparison of time required to compute y and search for x for the y as you choose larger and larger size p. Try to construct your own one way functions using only hand calculation on your mobile calculator.

1.2.1 Encryption function or a Trapdoor OWF (TOWF)

We now define a TOWF. Let X, K be sets of strings of bits and Y another set. A function $F : X \times K \to Y$ is said to be a TOWF with trapdoor K if

1. for any k in K the function $f_k = F(., k) : X \to Y$ is a OWF and is one to one.
2. Given k in K and a y in Y producing x such that $y = F(x, k)$ is easy.
3. Given a pair x in X and y in Y such that $y = F(x, k)$ for some k in K, producing any bit of k is difficult even with the knowledge that such a k exists. Here the argument k of F is called the *key* of the TOWF and K the key space.

The condition that $f_k(.)$ is one to one can be relaxed by stating that the number of distinct solutions x for any given y is very small (or the intended solution is recognizable by another OWF called a hash function). Like the relative OWF we can consider the relative provable TOWF by modifying above definition to conditions of relative provable OWFs.

Excercise 6. This exercise requires background of Linear Algebra. Let A be an $n \times n$ nonsingular matrix over the binary field $GF(2)$. Let N be the smallest positive number such that $A^N = I$ called the order of A. Given two vectors u, v in $GF(2)^n$ such that $v = A^k u$, consider the exponential like function, $v = F(k, u) = A^k u$. Is this a practical TOWF with trapdoor k?

Excercise 7. This excercise is a research direction. Consider the problem of constructing TOWFs. A practical way of designing a secure encryption is to construct a good TOWFs. What are model problems of computation suitable for such application? One direction which may be explored is to construct such functions $f(x)$ such that the forward problem of computing $y = f(x)$ is at most $O((\log |X|)^3)$ while the reverse problem of computing all x from y is an approximation of a NP problem such that the problem is solvable in provable polynomial time of the order $O(\log |Y|^m)$ for $m >> 3$.

1.2.2 Secure communication using TOWF : Symmetric key cryptography

We now see how a TOWF can be used to achieve confidentiality that is how Alice can confidentially communicate with Bob. Let $E : \mathcal{P} \times \mathcal{K} \to \mathcal{C}$ be a TOWF with K as key space where $\mathcal{P}$ denotes the space of messages (or plaintexts) and $\mathcal{C}$ that of ciphertexts. Alice and Bob undergo following protocol

1. Alice and Bob agree on (or exchange) a key K in $\mathcal{K}$ prior to communication.
2. Alice computes $C = E(P, k)$ in $\mathcal{C}$, for P in $\mathcal{P}$ and sends to Bob over an insecure channel.

3. Bob computes P given C using K which is equivalent to computing the function $D(.,.)$ given its arguments C, K. $D : \mathcal{C} \times \mathcal{K} \to \mathcal{P}$. Thus the function $D(K,.)$ inverts the encryption function $E(K,.)$ as the following relation holds:

$$x = D(K, E(K, x)) \tag{1}$$

The communication is secure owing to the fact that even if C is available to an intruder over the insecure channel, P is difficult to obtain without K since $C = E(P, K)$ is a OWF for any K. Similarly since K is the trapdoor, computing the decryption P given C and K is easy. But the problem of computing any bit of K is difficult given both P and C. The TOWF or the algorithm $E(.)$ is called the *encryption* algorithm the algorithm $D(.)$ is called the *decryption* algorithm. The key for encryption and decryption is same hence this method is called *symmetric key* cryptography.

Remark 1. Why is the third condition of the TOWF then required in secure communication? Further, it follows that k has to be exchanged securely by Alice and Bob prior to communication. In other words this means that to communicate securely over insecure channel requires a secure channel for key exchange.

Excercise 8. X and Y denote set of all strings of bits of lengths m, n respectively. If $F : X \to Y$ is a OWF, construct a trapdoor OWF $E : X \times Y \to Y$ with trapdoor X.

1.2.3 Indistinguishability of encryption

In practical use of encryption, an encryption algorithms is often required to satisfy a different security condition. This is known as *indistinguishability*. When we say that the encryption function has $E(., K)$ as a OWF for every K it is meant to be difficult to compute P from $C = E(P, K)$. But instead of computing P indistinguishability requirement of confidentiality is that an intruder who has selected two different P_1, P_2 is unable to distinguish which P_i is encrypted given a ciphertext C.

1.3 Attacks on encryption

By attack we mean a way to subvert the symmetric encryption protocol above by which confidentiality can be compromised. We can consider following ways to subvert the above protocol. First, an important assumption is made that, the encryption and decryption algorithms (or the mechanisms) of producing C given P, K or P given C, K known known to the intruder. In any specific attack, the intruder never has the knowledge of K but the intruder can ask for C for any chosen P or can ask for P for a chosen C. This assumption follows from the Kerkhoff's principle which is discussed below.

1. Key exchange channel attack called *man in the middle* attack. An intruder subverts the security of the key exchange and distributes keys k_a, k_b to Alice and Bob respectively.

2. Known plaintext attack. Intruder knows ciphertext C of some known plaintexts P for the same key K. If enough number of such (P, C) pairs for same key are available the encryption is weakened as the problem of guessing bits of K may become easier.

3. Chosen plaintext attack. The attacker is able to choose P for which the pairs (P, C) for the same key K makes computation of bits of K easier. This can be enhanced by considering adaptively chosen plaintexts from a previously known ciphertext.

4. Chosen ciphertext attack. Intruder chooses C and gets it decrypted to get P such that sufficient number of such pairs make the guessing of bits of K easier. This can also be enhanced by adaptively chosen ciphertexts from a previously obtained plaintexts.

5. Ciphertext only attack. This is the hardest cryptanalytic problem. In practice any cipher which allows solving bits of either P or K given only C is considered dangerously weak.

Goal of cryptanalysis is not only to break cryptographic schemes of adversaries but also to estimate the security of our own cipher designs. The third condition of TOWF is necessary for achieving secure communication due to the reality of executing above attacks.

1.3.1 Kerchoff's Principle 1883

According to this principle security of a cipher $E(,)$ is not enhanced by secrecy of the algorithm $E(.,.)$ or $D(.,.)$. The security should be solely dependent on choice of K in $\mathcal{K}$ (and its size). Kerkhoff wrote following guidelines for use of encryption for military purpose [1][1] We can translate these practical guidelines in the framework of OWFs as follows.

1. Encryption and decryption mechanisms or the algorithm should be easy for implementation or easy for computation.

2. The security of encryption (difficulty computation of P from C without the knowledge of K, or that of bits of K from the knowledge of (P, C) pairs) should be solely dependent on the length and secrecy of the key. Security of encryption should not be compromised even if details of implementation of the cipher or the cipher algorithms E or D are leaked.

It also implies that there should be no constraints on the choice of key K or that any K can be chosen randomly from the key space. By this principle the security of the encryption should solely be the property of length of K or the number of information bits used in representing K as long as no further information about K is known. Lack of knowledge of key K can be equivalently considered as true randomness in the choice of K.

Goals of cryptanalysis are therefore to

[1]Here system refers to the encryption mechanism or the algorithm.

1. The system must be substantially, if not mathematically, undecipherable;
2. The system must not require secrecy and can be stolen by the enemy without causing trouble;
3. It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants;
4. The system ought to be compatible with telegraph communication;
5. The system must be portable, and its use must not require more than one person;
6. Finally, regarding the circumstances in which such system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.

1. Estimate the minimum size of key which is adequate for security of encryption by a TOWF and forecast of computational technology in a foreseeable future.

2. Estimate the number of encryption sessions that can be carried out by same key without compromising the security of encryption. Alternatively, estimate the age of the cryptosystem.

3. Estimate the difficulty of subverting the TOWF by side channel information.

The minimum size (in bits) of the key decides the difficulty of brute force search. Data on number of sessions encrypted using the same key will give an information on the statistical biases of the TOWF making guesses on bits of plaintext and key more probable. Side channel information such as amount of time taken to encrypt and decrypt, trace of amount of power or current consumed during encryption or radiation emitted or any information on internal processes of the mechanism measured from the surrounding can be utilized in weakening the functionality of the TWOF.

During WWII the breaking of the German cipher Enigma is estimated to have shortened the war by at least 5 years. The break of Enigma happened mainly because the keys used for encryption were not chosen randomly. For instance the protocol for entering keys in the enigma machine required that the key had to be retyped for confirmation. Hence the key was fixed by only half of the symbols used from any one end. There were also biases involved in producing the ciphertext due to commonly repeated symbols in multiple keys. These were discovered. Finally, Enigma did not strictly follow Kerchoff's principle. The German designer who designed Enigma was bribed and allowed Polish army to photograph the construction details of the machine which facilitated its breaking. Illuminating discussions on Enigma break are available on Internet and the book by Simon Singh [2].

Remark 2. It is important to realize that Kerkhoff's principle DOES NOT IMPLY that ciphers used by a Government agency should be made public. The principle means that knowledge of the cipher algorithm should not be a weakness of encryption. In several known situations a secret cipher algorithm was disclosed by unexpected situations and reverse engineering. Hence secrecy of the algorithm is not a realistic assumption for security.

Excercise 9. Determine real life situations in which the above cryptanalytic attacks can be carried out on an encryption scheme.

Excercise 10. Construct examples of TOWFs and physical mechanisms by which such functions can be realized.

1.4 Data integrity

Possibility of chosen plaintext and ciphertext attacks amount to a possibility of inserting changes in plaintext and ciphertext from the intended plaintext P and the associated ciphertext $C = E(P, K)$. Given such a possibility it follows that only confidentiality is not enough to detect whether there has been a tampering of the message. The cryptographic channel is said to have *data integrity* if there is a mechanism along with encryption by which the receiver can ascertain such a tampering of the original plaintext or the ciphertext of the plaintext. Data integrity can be achieved in symmetric key cryptography by using a

OWF called *hash function*. However this function must satisfy additional requirements of collision resistance.

Let $H(.)$ (which produces a fixed length strings from arbitrary strings) be such a hash function. Alice encrypts P along with a hash of the message $h = H(P)$. The value h is also called the message authentication code (MAC). When Bob decrypts he computes (possibly tampered) $\tilde{P}$ whose hash $\tilde{h} = H(\tilde{P})$ cannot match h unless $P = \tilde{P}$ or the encryption is un-tampered. Hash function must therefore satisfy

Definition 1. Collision resistance property: A hash function $H(.) : \{0,1\}^n \to \{0,1\}^m$ is said to be *weakly collision resistant* if given a string h in the range of H and an input x such that $h = H(x)$ it is difficult to find another input $\tilde{x}$ such that $h = H(\tilde{x})$, and *strongly collision resistant* if is difficult to compute strings x, $\tilde{x}$ such that $H(x) = H(\tilde{x})$.

We shall see later how a hash function can be practically realized using OWFs. Hence construction of good OWFs can practically resolve the problem of meeting requirements of confidentiality and data integrity using symmetric key cryptography as long as a secure channel is available for key exchange.

1.5 Public key cryptography

Symmetric key cryptography poses following difficulties in its use.

1. Exchange of the symmetric key requires a secure channel. This has high cost, delays and risks.
2. Two entities who have never exchanged information before cannot utilize symmetric cryptography.
3. Number of keys required for n users of symmetric key grows as $O(n^2)$.
4. The serious mishap in which key is shared with a wrong party (called Man in the Middle attack) requires authentication of the data origin or identity. This cannot be fulfilled by data integrity.

Hence key exchange and authentication arise as two most important problems of symmetric key cryptography and are addressed by public key cryptography. Advent of public key cryptography has also led to development of *signature* which satisfies the requirement *of non-repudiation* in information transaction. This way modern cryptography has potential to offer following requirements in information transaction

1. Confidentiality.
2. Data integrity.
3. Key exchange over a public channel.
4. Authentication of identities.
5. Non-repudiation.

Functional realizations of Public Key cryptography in practice has been achieved under unproved TOWFs. Public key cryptography also has a model for solving the problem of confidentiality without need for key exchange by creating public and private keys. However then the key exchange requirement is replaced by trust on an entitiy who guarantees binding the public keys to identities. This later problem is practiaclly resolved to some extent by signature and certificates. Recent developments in digiatl currencies have utilized a protocol known as *blockchain protocol*. Blockchain has a model for trust, networks of trusts and trusted parties.

1.5.1 A functional description of a Public key encryption scheme

Consider a function $E(K, x) : K \times X \to X$ with following properties

1. $E(U, x)$ denoted $E_U(x)$ is a OWF. U is called the public key.
2. $y = E_U(x)$ has inverse function $x = D(R, y)$ denoted $D_R(y)$ such that
$$x = D_R(E_U(x)) \forall x \in X \text{ and } y = E_U(D_R(y)) \forall y \in X$$
3. $D(R, y)$ is a TOWF of y with trapdoor R. R is called the private key.
4. The function which generates the public key $U = H(R)$ from the private key is a OWF. There is a unique R corresponding to U.

With the help of such functions $E(.,.)$, $D(.,.)$ and $H(.)$ a public key encryption scheme can be created by the following protocol, for sending an encrypted message P to Alice: Alice is a member of the group which uses functions $E(.,.)$, $D(.,.)$, $H(.)$ which are known publicly.

1. Alice chooses the private key RA and generates the public key UA and makes UA public. RA is the associated unique private key of Alice.
2. Bob requests for the public key UA of Alice or reads from a public database.
3. Bob computes the ciphertext $C = E(UA, P)$ and sends to Alice over a public channel.
4. Alice recovers
$$P = D(RA, C)$$

Since $E(UA, .)$ is a OWF, computation of P from known C is infeasible for intruder Eve. Computation of RA knowing UA is also infeasible since $H(.)$ is a OWF. Next, since there is unique RA for a known UA, only Alice can decrypt C to get P. This way Bob can send message P to Alice over public channel without having exchanged key with Alice. However Bob must be sure that the entity whose public key is UA is indeed Alice. Hence this public key encryption scheme requires an authority which can authenticate the public key of Alice. This is possible with the help of a signature scheme

1.5.2 A functional description of a Public key scheme for key exchange

There is another scheme in which key can be exchanged over a public channel. Requirements of this scheme can be explained in terms of two finctions $\phi(.)$ and $\psi(.,.)$ as follows:

1. R and U are two sets of large cardinality such as $\{0,1\}^n$
2. $\phi : R \to U$ is a OWF.
3. $\psi : R \times U \to \{0,1\}^*$ is a TOWF with trapdoor R.
4. ϕ, ψ satisfy following identity which can be called as weak commutativity on R

$$\psi(R_a, U_b) = \psi(R_b, U_a) \forall (R_a, R_b) \in R \times R$$

which is equivalently the identity

$$\psi(R_a, \phi(R_b) = \psi(R_b, \phi(R_a) \forall (R_a, R_b) \in R \times R$$

which is a form of weak commutativity between a and b. Using these functions Alice and Bob can carry out key exchange over a public channel by following protocol:

1. Alice and Bob choose private keys a, b in R respectively independently.
2. Both announce public keys $\phi(a)$ and $\phi(b)$ in U.
3. Both compute the common quantity

$$S = \psi(a, \phi(b)) = \psi(b, \phi(a))$$

called shared key.

Excercise 11. Describe "man in the middle attack" on the key exchange scheme.

Both the public key schemes have been realised by mathematical functions. Several other types of functional descriptions have been found for realizing public key cryptography. However successful mathematical realizations of such functional descriptions from the point of view of security of the (T)OWFs are very few.

Excercise 12. Construct (T)OWFs to realize the two public key schemes

Excercise 13. Construct a functionality of a public key encryption scheme using the functionality of the key exchange scheme

1.5.3 Signature scheme from PK encryption scheme

Consider given a public key encryption scheme as above by specifying the TOWFs E and D. Suppose Alice has private, public key pair (R_a, U_a). Alice can sign a message M as follows:

1. A message encoding function μ is given which produces $m = \mu(M)$ in X

2. Alice signs by computing $y = D_{R_a}(m)$ the signature on M.

3. To verify signature on M by Alice, Bob computes m from the known message M. Then computes $E_{U_a}(y)$.

$$E_{U_a}(y) = E_{U_a}(D_{R_a}(m)) = m$$

Having the result m correctly gives verification that Alice signed the message M.

Excercise 14. Construct a funactionality of a signature scheme from the key exchange scheme

1.6 Present state of application of cryptology

Cryptography cannot be used without cryptanalysis or an assurance of security. Many modern cryptographic functionalities have been realised under unproved security estimates. However they are believed to have strong levels of security. Modern cryptography has demonstrated useful applications to diverse areas such as E-commerce, secret sharing, zero knowledge proving, E-voting, digital cash etc. and is a science of strategic importance. While the technology of cryptanalysis is rapidly evolving, modern ciphers and cryptographic schemes are not expected to be breakable with present day technology or within a foreseeable future. However key lengths required to offer security have also reached their limits in terms of performances of cryptographic algorithms. Hence hardware technology for acceleration is increasingly playing a major role in cryptographic implementation.

A major advance in cryptography is expected to be in computational speeds with high levels of security by utilization of parallel computation. Similarly several new applications in information transaction shall pose challenges for cryptography for which solutions shall be developed using existing schemes.

2 Information theoretic security, security at the physical layer of communication

In the classical cryptography discussed above, notion of security is in the formalism of computational security of its primitives. This notion of security is based on apparent computational difficulty of solving some of the challenge problems such as NP complete problems, factorization of long integers, discrete logarithms over elliptic curve groups, word problems on groups etc. Although for the current sizes of keys there appears no danger to their security these schemes have some disadvantages as follows:

1. Require up-gradation of key length with advances in cryptanalysis.

2. They will soon start becoming impractical in performance due to large key lengths.

3. Are not directly appropriate and convenient for implementation at physical layer infrastructure of communications systems and networks.

For achieving cryptographic services at physical layers arithmetic suitable to physical layer operations and cryptanalysis based on physical signal coding scheme are necessary. Alternatively, simultaneous cryptography and coding of information will be desirable.

An alternative proposal for security is that of schemes which depend on the coding used for the channel and information theoretic notion of security. These schemes are based on codes which can achieve capacity for secrecy. However these schemes also have disdvantages such as

1. Public key schemes are not available. McEliece scheme is a public key scheme based on principle of error correction coding but is not yet suitable for physical layer.

2. Depend on assumptions about channel and messages as well as relative capability between authentic and intruder entities in estimating the channel which may not be realistic. (A common assumption that the intruder has lack of knowledge of the channel relative to authorized users is equivalent to having a secret symmetric key).

3. Simultaneous coding and encryption is not yet established.

2.1 Information theoretic analysis of security for symmetric cryptography

In a paper in 1949 Shannon [12] defined a notion called *perfect secrecy* for establishing security of symmetric key cryptography and proved that the Vernam one time pad had perfect security. This notion of security was defined in terms of information theoretic analysis of probability distribution associated with the plaintext and its transformation due to enciphering by a key. Shannon's theorem allows one to establish correspondence of TOWFs with the distributions of plaintexts and those induced on key space and ciphertext space.

Information theoretic description of the situation arising due to an encryption function is as follows. Let $\mathcal{K}, \mathcal{C}, \mathcal{P}$ denote the spaces of key, plaintext and ciphertext and $E : \mathcal{K} \times \mathcal{P} \rightarrow \mathcal{C}$ be an encryption function. A plaintext P is a singleton event in $\mathcal{P}$ with probability distribution $pr(P)$ and for a fixed K in $\mathcal{K}$ the encryption function induces a distribution $p(C)$ on $\mathcal{C}$ as a function of event P . Similarly when a ciphertext C is given, with plaintext P as an event in $\mathcal{P}$ there is a distribution denoted $pr(K)$ for key K to satisfy the relation $C = E(K, P)$. Finally $p(P, C)$ denotes the joint probability distribution of the event that P is the plaintext and C is the ciphertext for some key. Given these distributions there is the conditional distribution $p(C|P)$ which is the conditional probability of the event P occurring given the ciphertext event C for some K.

2.1.1 Perfect secrecy

Shannon defined perfect screcy as a property of encryption. The encryption function E is said to have perfect secrecy if

$$p(C|P) = p(P)$$

Perfect secrecy thus implies that given the ciphertext C, this event given no knowledge about the event of P occurring other than what is already known about distribution of P.

This can be alternatively explained in terms of entropy of the plaintext space $\mathcal{P}$ and joint entropy with $\mathcal{C}$. The uncertainty associated with the plaintext is denoted by the entropy

$$H(P) = -\sum_{P \in \mathcal{P}} p(P) \log p(P)$$

The joint entropy with the ciphertext distribution at a fixed K is given by

$$H(P, C) = -\sum_{P,C} p(P, C) \log p(P, C)$$

The conditional entropy given C at this K is defined by

$$H(P|C) = H(P, C) - H(C)$$

Then perfect secrecy has an equivalent definition, E has perfect secrecy if

$$H(P|C) = H(P)$$

at this K and all possible keys K which satisfy the identity $C + E_K(P)$. This condition can also be written in terms of mutual information. For the distributions of events P, C explained above at a fixed K the mutual information between P and C is defined as

$$I(P, C) = H(P) + H(C) - H(P, C)$$

Hence perfect secrecy of E also means that $I(P, C) = 0$

2.1.2 Shannon's theorem

Shannon's theorem allows a glimpse into the relation of perfect secrecy to the TOEF property of E in terms of the distribution of K. We may state a restrictive version of this theorem

Theorem 1. Let $|\mathcal{K}| = |\mathcal{P}| = |\mathcal{C}|$ then the following statements for an encription function $E(K, P)$ are equivalent

1. E has perfect secrecy relative to the distributions of P, C defined above.
2. For a fixed C the distribution of K is uniform. Hence $p(K) = 1/|\mathcal{K}|$.
3. $H(K) \geq H(P)$

For the proof of first two statements see [4]. Proof of the third statement is available in [5]. Following corollaries show practical relevance of this result

Corollary 1. Under the assumption that E_K has perfect secrecy

1. If P involves m alphabets then K must have at least m alphabets.
2. The Vernam one time pad has perfect secrecy.

The second statement of above theorem has implication for the TWOF proprty of E. Since under the perfect secrecy assumption K is uniformly distributed, given a plaintext ciphertext pair (P, C) a probability of hitting a correct key to satisfy $C = E_K(P)$ is decreases exponentially with size of the key space. However this does not imply that computational problem to solve K from this relation is "difficult". On the other hand even if this problem is "difficult" it does not imply that $I(P, C)$ is small. These two notions of security of E have thus independent foundations.

2.2 Physical layer security

Traditional cryptography does not consider the physical channel which has inherent noise and capacity. Shannon's definition of perfect security considers noiseless channel for transmission of ciphertext. Models for secure communication over physical channel that can be considered are

1. Wiretap channel of Wyner. The transmitted symbol X by Alice is received as Y by authentic party Bob and as Z by intruder Eve. The probability of error p_E at Eve is higher than p_B at Bob, $p_B < p_E$. The symbol X is encoding of the symbol S. Goal of coding is to maximize the equivocation $H(S|Z)$ together with maximizing the information $I(S, Y)$ transmitted. Thus in the wiretap channel information received by Eve is degraded relative to Bob.

2. Alternative model is that the encrypted information S is transmitted through a noisy channel and is available to both Bob and Eve equally likely. Hence we can assume that there is no wiretap required for Eve. However there is additional information available with Alice and Bob relative to Eve about the channel which is equivalent to secret key bits. This secret key K is used for coding S. Knowing K Bob should have advantage in decoding and deciphering Y to recover S. Not knowing K Eve should in principle be left with only choice of trying all bits of K by brute force to recover S. This is analogous to symmetric key encryption and is also the model of simultaneous encryption and coding.

3. Third model is of a channel over which each user keeps beeping public codes for information transmission. Alice who accesses the public information can verify authenticity of the owner Bob of his public code and use the code to encrypt information sent over the channel. We expect only Bob to be able to decrypt despite the channel noise. Eve may at most be able to correct errors and decode the information till the ciphertext. This is equivalent to public key encryption using simultaneous encryption and coding.

4. Another model for security (but perhaps not cryptography) over physical channel is being proposed withthe help of polar codes. It was shown in [11] that as the code length increases the channels such as BSC undergoes the phenomenon of polarization. This makes some of the channel lines very poor for decoding as compared to others. This is used for discriminating between reliable channels used for more secure communication as compared to unreliable channels.

Hence in the second model of secure communication over physical channel the scheme for coding S depends on secret key K. The decoding (generally) as well as decryption specifically should be dependent on K. Information theoretic security is also developing fast. A comprehensive account is available in [10]

References

[1] http://www.petitcolas.net/fabien/kerckhoffs/

[2] Simon Singh, Code Breakers, Fourth Estate Publishers, London, 1999.

[3] Waade Trape and Lawrence Washington, Introduction to cryptography and coding theory. Pearson 2006.

[4] Johanne Buchmann, Introduction to cryptography, Springer, 2006.

[5] Serge Vaudeney, Classical introduction to cyptography, Springer, 2006.

[6] Bruce Schneier, Applied Cryptography, John Wiley, 2002.

[7] A. Menezes, van Oorschot, Vanstone, Handbook of applied cryptography, CRC Press 1997.

[8] D. Stinson, Cryptography, Theory and practice, CRC Press, 2005.

[9] W. Mao, Modern Cryptography, Printice Hall, 2004.

[10] M. Bloch and J. Barros. Physical layer security. Cambridge University Press, 2011.

[11] E. Ariken. Channel polarization: A method for constructing capacity achieving codes for symmetric binary input memoryless channels. IEEE Trans. on Info. Theory, vol.55, no.7, 2009.

[12] C. E. Shannon, Communication theory of secrecy systems. Bell Systems Technical Journal, vol 28, pp.656-715, 1969. Re-edited in Claude Elwood Shannon-Collected papers, IEEE Press, New York, 1993.