CRYPTOGRAPHY

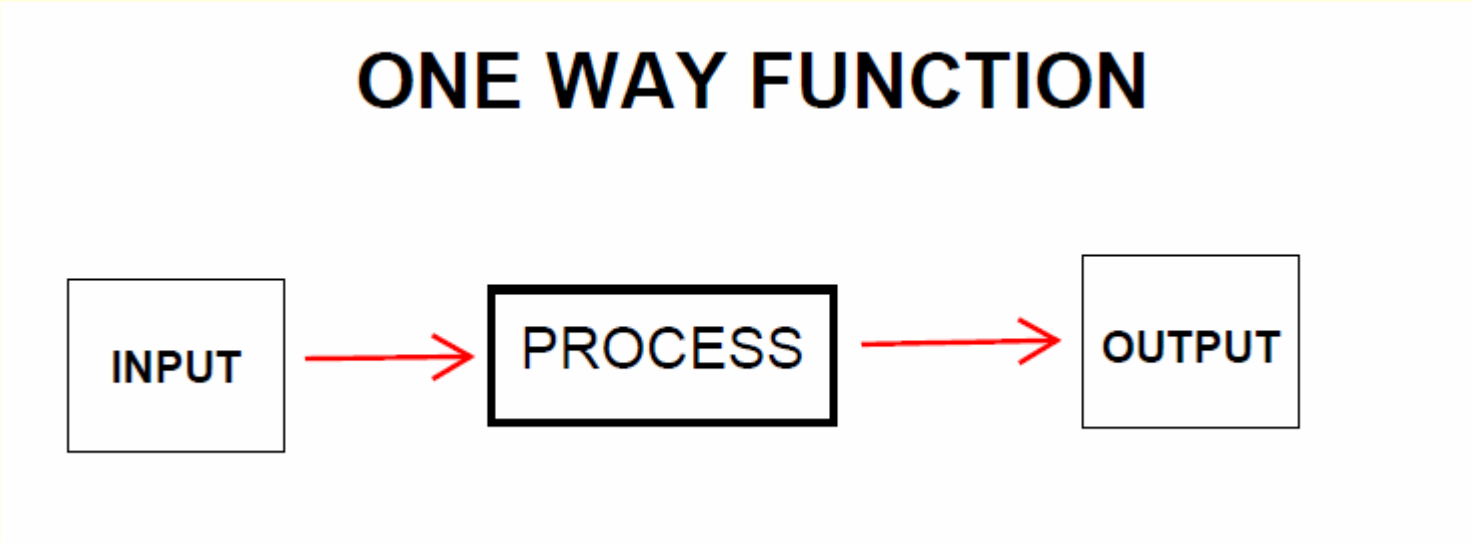
Security Products

Introduction

- **Objective** : As the country moves to digital, cryptography will play a role in it.
- Cryptography is a wide field and evolving from “security as a layer” to “security products”. The opportunity for crypto based security products is huge as Cryptography can introduce fine controls for **identification, authenticity, accountability**.
- **Credit cards**

INFORMATION SECURITY

- **Two pillars of Information Security : Confidentiality and Integrity are implemented in cryptography.**
- **The basic primitive of crypto is the one way function which simply means that one can compute output very easily given the input but cannot reverse it.**

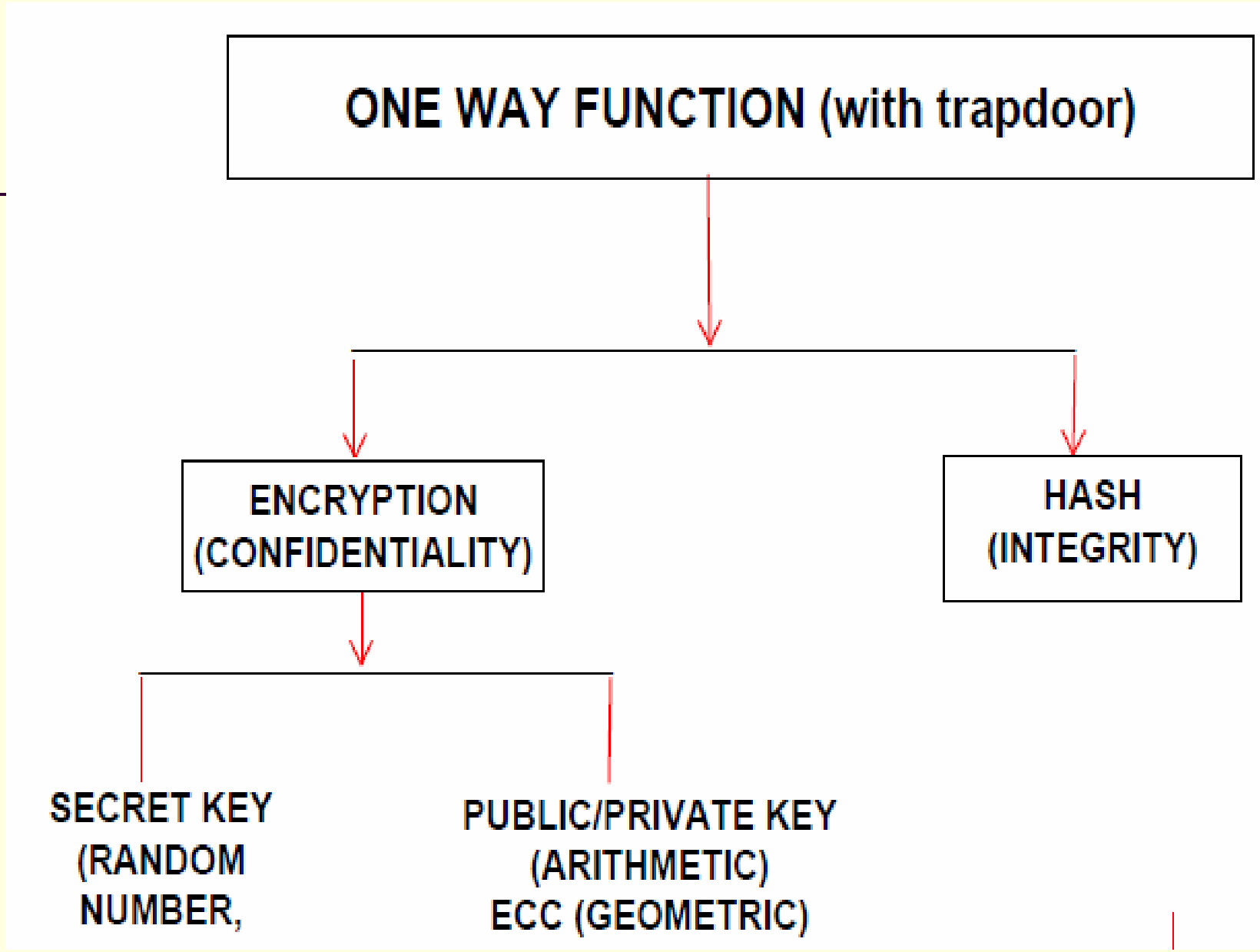


INFORMATION SECURITY

- **one way function i**s hidden in all crypto functions all encryptions can be looked upon as a OWF.
- One way functions can be implemented through application of modular arithmetic, XOR logic, group operations, scalar multiplication and randomness.

INFORMATION SECURITY

- Cryptography exploits one way function to transform text (encryption) **Confidentiality** and calculate a hash of a message. (**INTEGRITY**)
- Crypto achieves solutions for **Integrity** by producing a hash of a message by a multi step process.


ONE WAY FUNCTION (with trapdoor)
ENCRYPTION (CONFIDENTIALITY)
HASH (INTEGRITY)
SECRET KEY (RANDOM NUMBER,
PUBLIC/PRIVATE KEY (ARITHMETIC) ECC (GEOMETRIC)

Security Tenet (Confidentiality)

Basic security tenet is that given a ciphertext for an attacker it should not be computationally feasible to know anything of the plaintext.

Given ciphertext of Plaintext : Meet me at 5 PM

1. Evasedroping : Meet me at 5 PM

2. Modify/Alter text : Meet me at 7 PM

3. Change the text: Please Go Home

Security Tenet (Integrity)

- Crypto achieves solutions of **Integrity** by producing a hash of a message by a multi step process
- Given ***only*** hash value of a message find **the message** which hashes to the same value.

Given hash *4bc48e00300464d2670958ab3c8982ea* of a password "india123". Find the password "india123"

- Given **hash *4bc48e00300464d2670958ab3c8982ea* of password and password "india123"** find another password which hashes to the same value.
- Find a pair of passwords 'p' and 'p1' chosen at random which hashes to same value 'h'. (Birthday Attack)

What is THE **SECRET**?

- In crypto prime number is THE SECRET. The security of crypto is based on the fact that if you choose a large prime number then it is difficult for the attacker to guess it.
- SECRET KEY – 40 digits or 128 bits
- RSA - 600 digits or 2048 bits
- ECC – 40 digits or 128 digits
- The following is a table which shows that for every human being on earth more then trillion prime numbers are available.

Number of Primes

Digits	Number of Primes
3	168
6	78498
9	50847354
12	37607912018
15	2984457042266 9
18	247399542877408 60

perfect secret system

- A Digital Cipher encryption system is *secure if no adversary can **compute** any function of the plaintext or the key from the ciphertext.*
- In a cipher system the only thing that can be kept a secret is the **key**. *The algorithms and designs are constantly under public scrutiny, and hence it is more likely that any problems will be uncovered at early stages.*
- The adversary always has some prior knowledge of the cipher systems in that if it is English language then he knows the frequency of the letters, there are common words, common combinations in English Language etc.
- By confusion and diffusion operations, redundancy and low entropy of English language is taken care of Confusion and diffusion achieved by substitution and permutation in multiple rounds in many security standards.
  - **Tag line : No matter what message you encrypt, the probability of getting a particular ciphertext is the same.**

Crypto Vs Risk Analysis

- Risk Analysis results in general are an input for evaluating and implementing security controls which can be implemented by crypto. Crypto controls are more effective and efficient.
- Generally RA recommends and Crypto implements.

Example :

- Password controls, Credit Card Data, TLS/SSH, File Integrity.

CRYPTO & SECURITY

- Cryptography is generally incorporated at design, upto chip level, stage and functionality is introduced afterwards or in parallel. In normal system environments security is an afterthought, or rather another peer to peer layer.
- Cryptographic controls are based on vigorous analysis, testing and game theory whereby all error/alerts messages are designed to prevent leakage; in networks error/alerts messages are communicated to a peer to peer layer.
- Cryptographic controls are also established at macro (system) level for good governance of IT.

Cryptography and Security Standards

- Storing, Transmitting and processing sensitive data in encrypted form
- File Integrity
- Audit Logs – events, configuration, vulnerabilities.
- Digital Signatures – Authentication
- Introduction of new security features
- Governance of IT security controls

Applications of Cryptography

- Secure communications (*https, WEP, GSM*)
- Encrypting of disk
- Protection of content (Recording Industry)
- User Authentication (Digital Signatures)
- File Integrity - PC's - downloading programs Vo
- QR codes, Boarding passes, RFID Tags
- Auctioning
- Voting

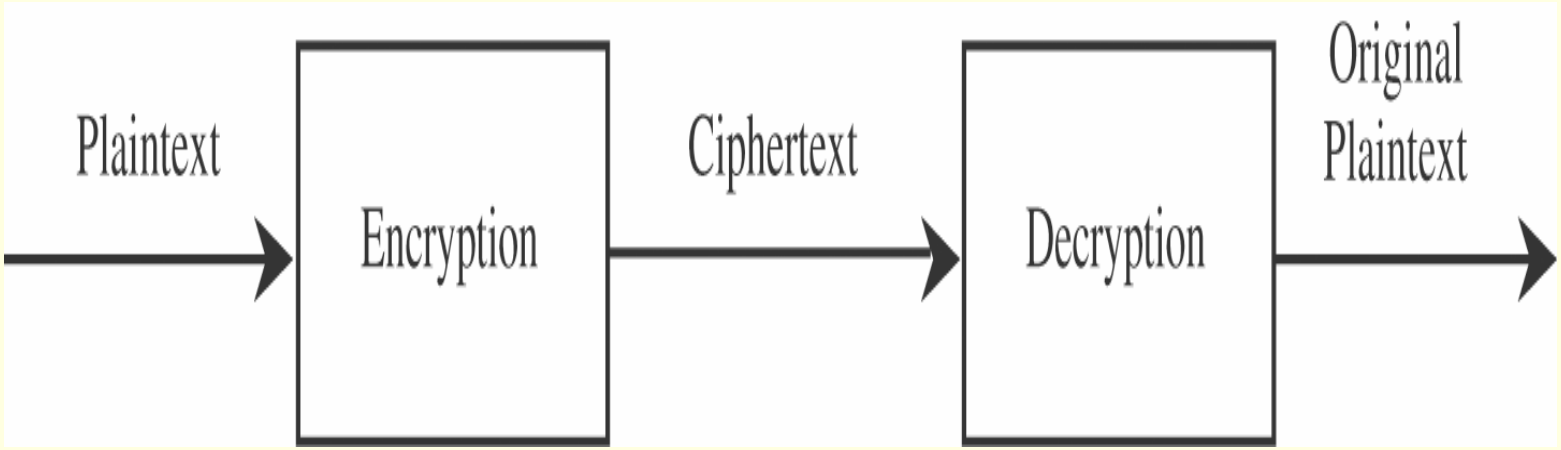
How to Learn Cryptography (Holistic)

- One approach is to read narrations about cryptography and novels where crypto is set in the background.
- There are many stories of codebreakers which have been documented. some are heroic. There is also a crypto song.
- A German cipher machine called Enigma which use to do multistep encryptions used during Second World War, (pre-digital) is a subject of many books and analysis.
- Dan Brown novels Digital Fortress, the Da Vincy Code crypto is set in the background.
- Stephen Levy, (How the code rebels beat the government) and Turing the Engima, the battle for the code are some other books,
- David Kahn's "The Codebreqkers", Simone Singh's "The Code Book" are historical treatments of cryptography

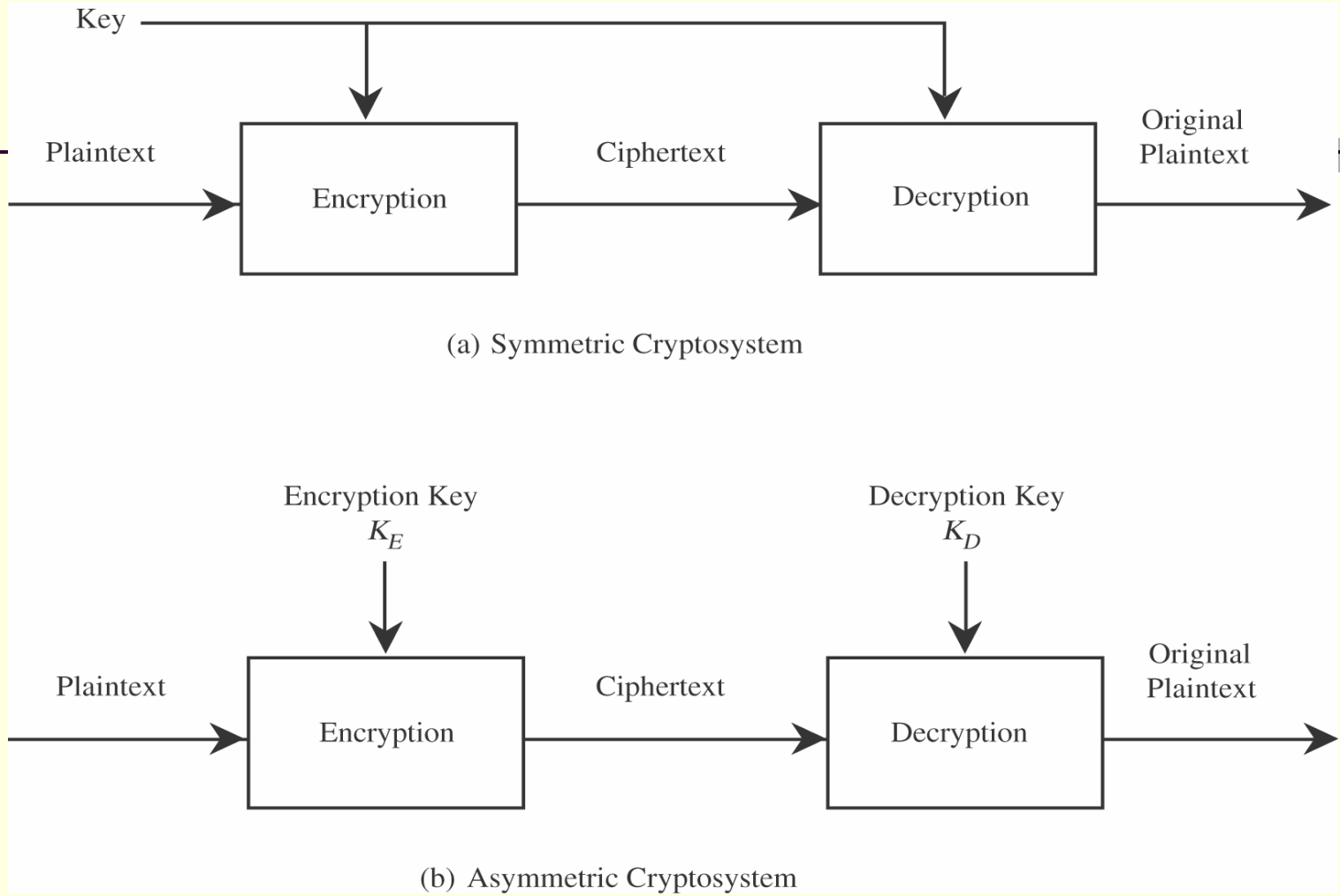
How to Learn Cryptography

- Cryptography is a parallel development of maths, logic and processes. From ancient times crypto was practiced by trained specialist but today it is becoming a requirement in many fields.
- Cryptography has evolved from transmitting data reliable to securely and then migration to store data at rest securely.
- Approach to understanding cryptography can be maths, logic or process oriented. Many believe that you should first learn maths then the logic, some believe that you should first learn the logic then maths, crypto protocols follow then these. As some may simply say first learn the process then the maths and logic.

Basics of Crypto



Encryption/Decryption



Encryption with Keys.

Basics of Crypto - (Pre Digital) Secret Key

- Initially Cryptography was practiced by shift, substitution, and then permutation and matrix transforms of text. With the advent of Computers these transforms got complex and scaled up during the Digital Age, randomness was added and also multiple and iterated transforms were introduced.
- A standard Crypto system achieves diffusion, confusion by taking a combination of the procedure – shift, substitution, permutation and transform. A matrix transform achieves the goal that every bit of cipher text is dependent on each an every bit of plaintext.
- Digital Age also added Xor logic which has made crypto practical or available on desktop.

Basics of Crypto – Shift - Substitution

- **Shift cipher** – shift register (left, right) The alphabet has 26 letters and the alphabet can be encoded from 0 to 25. By shift we add a constant ‘x’ to the code to have a new value.
- If x is 5 then A is 5, B is 6 and Z is 4 and not 30
- plaintext letter: a b c d e f g h i f k l m n o p q r s t u v w x y z
- ciphertext letter: f g h i f k l m n o p q r s t u v w x y z a b c d e
- EXAMPLE
- **Substitution –** substitutes each letter in the alphabet with another letter from the alphabet
- plaintext letter: a b c d e f g h i f k l m n o p q r s t u v w x y z
- ciphertext letter: m n b v c x z a s d f g h j k l p o i u y t r e w q
- Substutution can become more complex if the pattern is changed periodically so that repeated text does not look the same.
- EXAMPLE
- In both of the above cases the shift or substitution key value is exchanged before transmission.

Basics of Crypto - **Permutation**

- **Permutatio**n : Here a text is divided into say blocks of ‘n’ characters and transposed according to a rule for example text “monsoons were heavy this year”
- *monso onswe rehea vythi syear*
- Suppose the transformation permutation is [5,1,2,4,3] text will be : *omosn eonws areeh ivyht rsyea – transformed text and the inverse is obtained by doing reverse 2,3,5,4,1.*
- ***Matrix transforms***

PUZZLE

- Given Ciphertext Find “keyword” plain text
- **WTOQ_IP_QTS_GSYWJMU_CJM_QTIP_FIKTSM**
- A bit of frequency analysis and thinking about common English words one can find the simple substitution:
- **WHAT_IS_THE_KEYWORD_FOR_THIS_CIPHER**
- Which is obtained using the substitution table:
- **ABCDEFGHIJKLMNOPQRSTUVWXYZ_**
- **OBFUSCATINGDEHJKLMPQRVWXYZ_**
- Hence the **KEYWORD** for this cipher is OBFUSCATING.

Basics of Crypto

- Modular Arithmetic – Addition, Multiplication, Exponentiation, Inverses
- Exclusive OR
- Dealing in integers of 300 digits (1024 bits) in Public key and 36 digits (128 bits) in secret key – all are prime numbers
- PseudoRandom functions
- Field operations –addition, multiplication, inverses of prime Numbers
- Calculator – MOD and XOR are standard functions
- Cipher - command line interface in windows
- http://www.cs.princeton.edu/~dsri/modular-inversion.html site for modular inversions.

Crypto (Modular arithmetic)

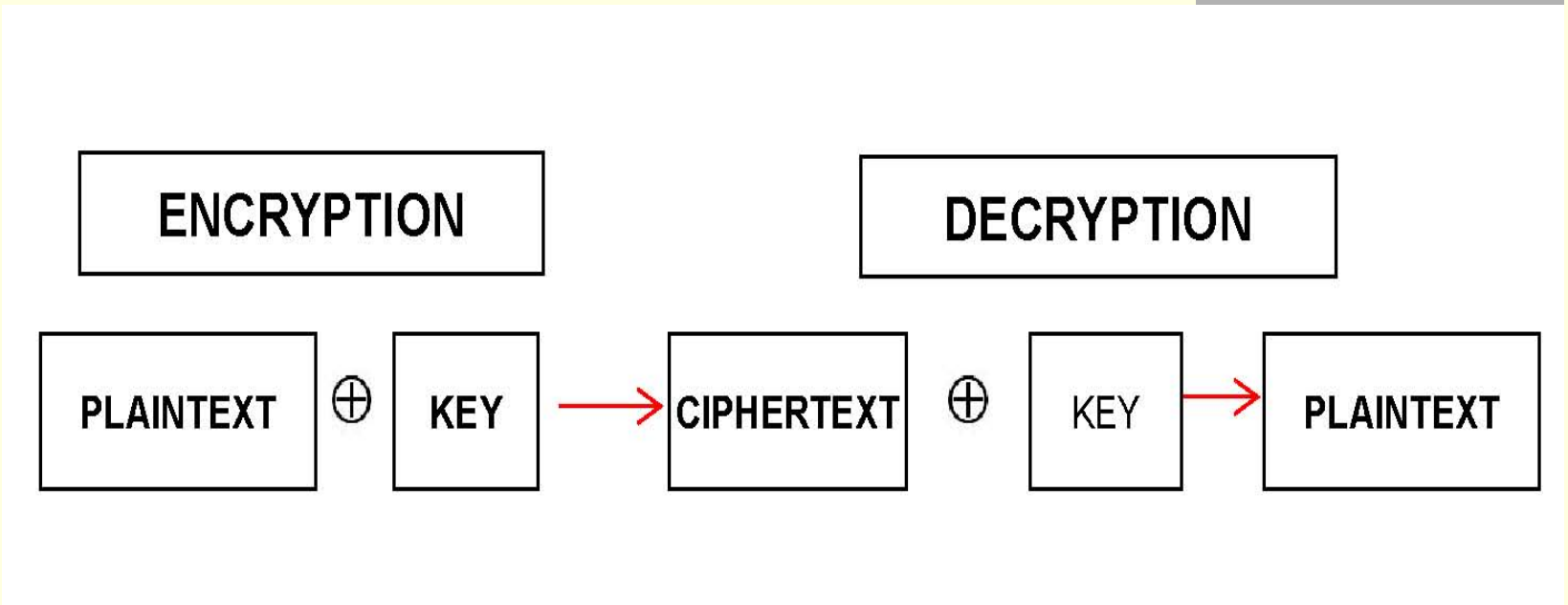
Clock & Calendar

Modular arithmetic is one of the basic input too.

- 7 plus 12 mod 10 = 9
- 7 plus 22 mod 10 = 9
- 7 plus 32 mod 10 = 9 but
- 7 minus 12 mod 9 = 4
- 7 plus 22 mod 9 = 2
- 7 plus 30 mod 15 = 7
- 4 mul 7 mod 23 =5
- 5 mul 7 mod 23 =12
- 7 mul 7 mod 23 =3
- 7 div 3 mod 23 = 7 mul 3^{-1} = 7 mul 8 div 23 = 10

Ex or $\oplus$ is MOD 2 operation

EX OR Logic ⊕


ENCRYPTION
DECRYPTION
PLAINTEXT
⊕
KEY
CIPHERTEXT
⊕
KEY
PLAINTEXT

Basics of Crypto(EX OR Logic ⊕)

Basically if ‘M’ exor (represented by ⊕) ‘K’ is equal to ‘C’,

‘M’ ⊕ ‘K’ ≡ ‘C’

Then *‘C’ ⊕ ‘M’ ≡ ‘K’.*

‘C’ ⊕ ‘K’ ≡ ‘M’

This ⊕ function is basically a ‘mod 2’ operation whereby the input bits are added and answer is the remainder (output) which is either ‘0’ or ‘1’ or (logically)

0001 ⊕ 1111 = 1110
0101 ⊕ 1111 = 1010
0011 ⊕ 1111 = 1100
1100 ⊕ 1111 = 0011
52 ⊕ 35 = 23 / m1 ⊕ k = c1
45 ⊕ 35 = 14 / m2 ⊕ k = c2
23 ⊕ 14 = 25 / c1 ⊕ c2 = m1 ⊕ m2
45 ⊕ 52 = 25

Encryption of Plaintext Bytes (Secret Key)

- Generate ***n*** random bytes to be additional plaintext bytes at the beginning of the sequence of plaintext bytes.
- Initialize an unsigned n-bit integer variable R to the encryption key.
- For each 8-bit byte, P, of plaintext (beginning with the newly added random bytes) execute the following :

a. Assign the high order 8 bits of R to a temporary variable, T.

b. P $\oplus$ T, producing a ciphertext byte, C.

c. Compute the next value of R (feedback) by the formula ((C + R) × c1 + c2) mod 65536, where c1 is 52845 (decimal) and c2 is 22719 (decimal).

Decryption of Ciphertext (Secret Key)

1. Initialize an unsigned 16-bit integer variable R to the encryption key (the same key as used to encrypt).
2. For each 8-bit byte, C , of ciphertext the following steps are executed:

a. Assign the high order 8 bits of R to a temporary variable, T .

b. C $\oplus$ T , producing a plaintext byte, P .

c. Compute the next value of R by the formula ((C + R) × c1 + c2) mod 65536, where c1 and c2 are the same constants that were used to encrypt.

3.Discard the first n bytes of plaintext; these are the random bytes added during encryption. The remainder of the plaintext bytes are the original sequence.

Modular Arithmetic (Inverses)

- In regular arithmetic the definition of inverse would be $a*a^{-1} = 1$ which is 25*1/25
- In modular the same definition applies but $a*a^{-1}$ mod n = 1.

  Example for n = 25
  - If a = 3 then $a^{-1} = 17$ so $a*a^{-1} = 51$ mod 25 =1 To calculate the inverse a formula exist called Euclidian theorem but a website also does it very conveniently.
  - http://www.cs.princeton.edu/~dsri/modular-inversion.html site does modular inversions conviniently.

Modular Arithmetic (Inverses)

- 2-13, 3-17, 4-19 are pairs of encryption and decryption keys in mod 25
- For mod 31 these pairs can be calculated to be

  9-7, 2-47, 2-109.
- The encryption (E) and decryption (D) key is defined over a mod value by the equation :

ED= 1 mod n

Construction of Encryption/Decryption Keys

- Modular inverses of mod 25 (2-13, 3-17, 4-19)
- Data is 5 and encrypted value is 5*2 = 10
- Decrypted value is : 10*13 mod 25= 130 mod 25 = 5
- Original text is 15 encrypted value is
- 15*2 mod 25 = 5
- Decryption 5*13 mod 25= 65 mod 25 = 15

RSA Algorithm (Public Key)

Choose two prime numbers :

- P = 71 and Q = 79
- 71*79 = 5609 : (PQ)
- (71-1)*(79-1) = 5460 : (P-1)(Q-1) - *Trapdoor*
- Choose a number 23 which is a prime and find its inverse 1187 (web site)
- 23 and 1187 are encryption/decryption keys
- If text is 135 the EC = 135^23 mod 5609 = 1367
- Similarly 1367^1187 mod 5609 = 135
- **In real practice the numbers p and q are derived by an iterated process from group theory**.

RSA Algorithm

- *IN the previous 23 can be private key and 1187 public key. The main strength is one cannot derive private key form public key.*
- *In real life RSA is 1024 bits - 300 digits long and the computation can be done only by special programs.*
- *RSA keys are used (Diffe-Hellman) to establish an exchange for secret key which is generally 128-256 bits long.*

RSA Algorithm

- In RSA the difficulty of factoring a large integer especially composite primes is considered to be HARD.

Secondly these groups are generated based on PRIME NUMBER Theory. RSA is much slower for both computation and bandwidth then secret key because of bit length in hardware it is 1000 times slower, so it is used for primarily to establish keys or signing where the overhead is low.

Some parameters in RSA

RSA is much slower for both computation and bandwidth then secret key because of bit length in hardware it is 1000 times slower, so it is used for primarily to establish keys or signing where the overhead is low.

Some parameters are :

- Time to encrypt
- Time to decrypt
- Number of one bits say to use a number like
- 65537 which is 1000000000000001 = 2^16 + 1

Example of key lengths (1970-2012)

- Q = 606938044258990275541962092341162602522202993782792835301301.
- (200-bit prime – in 1970)
- Q =

179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377678934248654852763022196012460941194530829520850057688381506823424628814739131105408272371633505106845862982399472459384797163048353563296242241371111. - (1024-bit prime- in 2012))

- Financial institutions are developing keys of 3072 bits to stay ahead in security.

Risks of crypto

- Risk analysis of crypto is called Cryptoanalysis. Besides the regular risks in using crypto like access control – physical, network crypto risks are redundancy, (Indian language) collisions, big maths, frequency distribution, timing or side channel .
- Testing of Crypto has not been standardised
- Crypto has issues of privacy, law and patents
- *More basically we are dealing in zeros and ones and the chances of guessing the value is always at least one half.*

Cryptoanalysis

- In a cipher system the only thing that can be kept a secret is the **key**. *The algorithms and designs are constantly under public scrutiny, and hence it is more likely that any problems will be uncovered at early stages.*
- The adversary always has some prior knowledge of the cipher systems in that if it is English language then he knows the frequency of the letters, there are common words, common combinations in English Language. If the plain text say is of a financial institution then he can expect common words in addition to above. An additional factor is that ASCII code length is 8 bits which can be encoded for 256 characters but only 96 characters are used.

CRYPTOANALYSIS

- For 8 bit ACCII code the uncertainty is about is about 37.6 for 256 bit keys
- Based on above parameters calculations have been done whereby redundancy of English language is .75.
- By confusion and diffusion operations, redundancy and low entropy of English language is taken care of Confusion and diffusion achieved by substitution and permutation in multiple rounds in many security standards.
- **Tag line : No matter what message you encrypt, the probability of getting a particular ciphertext is the same.**

Cryptoanalysis

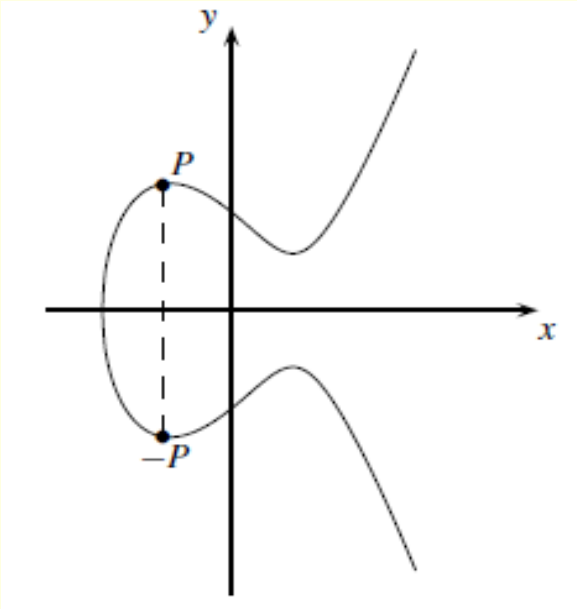
- ***No right security defination***
- ***One primitive multiple goals***
- How many queries do you need to find out the key ?
- Cost of the attack.
- Reduce complexities of an attack.
- We do nor get to know all security goals.
- Crypto should be designed to support applications and not other way around.
  - Nonce based
  - Industry has a lot of problems.
- Understanding System is the key.

Cryptoanalysis

- Linear analysis exploits correlation between linear combinations of bits of the state in different stages of encryption processes.
- Differential analysis exploits probabilistic propagation between bitwise differentiation of the state in different stages of encryption processes.
- Modern technology allows one to send millions of queries to a system and receive answers and the sender can send ciphertext or plaintext and receive answers.

ECC

- Elliptic Curve crypto is defined by an equation $y^2 = x^3+ax+b \bmod p$ and an infinity point.
- The shape of the curve is :



How did Elliptic Curves come into cryptography ?

- Elliptic curves, a type of equation whose highest exponent is three. Elliptic curves are one of the central objects in number theory.
- Elliptic curves have a long evolution and it is an algebraic equation whose solutions have come from geometric and topological fields.
- Elliptic curves under certain conditions from a finite field, and a cyclic group which will build a Discrete Logarithm Problem.
- Rational solutions of an elliptic curve form a group which can be used to generate crypto keys to be used for Encryption/Decryption.

Elliptic Curves and cryptography?

- ECC can be structured as having four layers
  - modular arithmetic
  - group operations
  - scalar multiplication
  - protocol layer.
- There is no known formula for finding rational solutions of an elliptic curve.

Elliptic Curves Cryptography

- It’s faster, more compact and more elegant than other public-key crypto.
- ECC is ideally suited for low power, low size applications. Its main application area is personal identification verification devices like credit cards, bio-metric cards etc.
- ECC is heavily researched topic in Cryptography and a lot of enhancements are expected in this field.

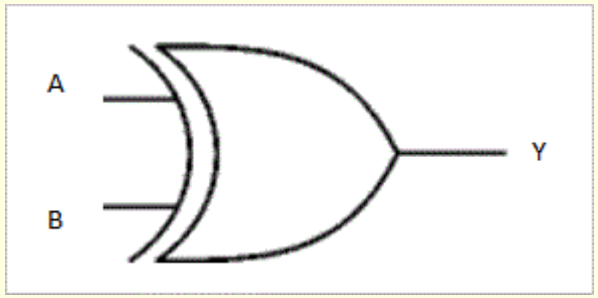
Elliptic Curve Equation

- $y^2 = x^3+ax+b \bmod p$

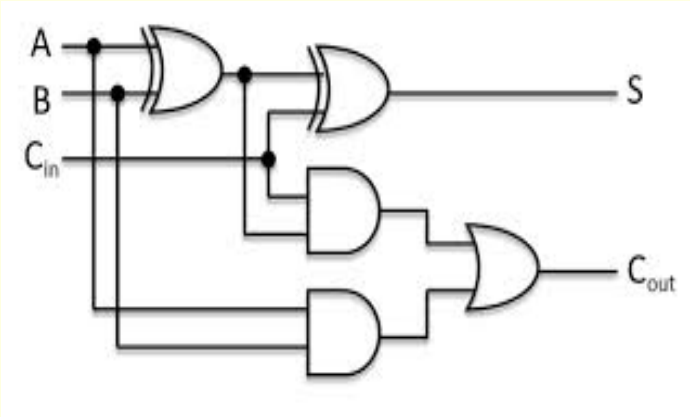
- P = 115792089210356248762697446949407573530086143415290314195533631308867097853951
- b = 41058363725152142129326129780047268409114441015993725554835256314039467401291
- #E = 115792089210356248762697446949407573529996955224135760342422259061068512044369

Advantage of ECC

- EX OR gate
- 1 bit add in binary fields



- 1 bit full adder



One way Hash functions

- Hash functions has many other names an some of them are message digest, fingerprint. (encoding of data) Hash function produces a fixed length output of a message.
- Hash Functions give integrity to a message.
- Some of the common Hash functions are MD5, SHA-1 which create MAC.
- One way Hash function with encryption key gives ‘Authenticated Encryption’.
- SHA1 algorithm produces a hash value by a 6-step process of padding of '1000...', appending message length, preparing 80 process functions, preparing 80 constants, preparing 5 word buffers, processing input in 512 blocks.
- Encrypting a message with 64 bit key creates a long document it is better to create a hash of the document which in turn is encrypted by a Digital Signature. By sending them independently “integrity” of message is maintained.
- Error rate of 160 bit hash is very low, DS is separate from the document and so on.

Password Hashing

- **Cryptographic Security** :
- **Defense against lookup table / TMTO Attacks**
- **Defense against CPU-optimized ‘crackers’** should offer only minimal speed-up improvements compared to those intended for validation (“slower for attackers, faster for defenders”).

  Defense against hardware-optimized ‘crackers’ The scheme should be ‘memory-hard’, that is, it should significant amounts of RAM capacity in a manner that cannot be optimized away through eg. TMTO attacks
- **Defense against side-channel attacks:** Password hashing schemes should aim to offer side-channel resilience. The second category of side-channel attacks we will take into consideration are so-called ‘memory leak’ attack

One way Hash functions (Prover & verify)

- **Modelling Hash & Prove (HP**) the idea of hashing and uploading data once and then using the resulting hashes across multiple verifiable computations. In this model, the verifier needs only to keep track of hashes, while the prover stores the corresponding data. The prover can use the data to perform computations and then (selectively) return results in plaintext to the verifier. Hashes yield several benefits when delegating verifiable computations.

Types of Cryptography systems

- Secret Key Cryptography (SK): Uses a single key for both encryption and decryption
- Public Key Cryptography (PK): Uses one key for encryption (public key) and another for decryption (private) (RSA, ECC)
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

Stream/Block Ciphers

- A collection of permutations over n – bit strings indexed by a secret key K
- Block Cipher operates on the input string in blocks of 64 bits. Block Cipher is the work horse of crypto. It is made up of **two algorithms**, E and D. These are encryption and decryption algorithms. Both of these algorithms take, as input, a key K. A block cipher takes an N bit plain text as input, and it outputs exactly the same number of bits as outputs. So it maps N bits on inputs to exactly N bits of outputs.
- Block ciphers are chained differently for achieving different applications. (CBC, CFB, OFB mode)
- Block ciphers operate on data with a **fixed transformation** on large blocks of plaintext data; stream ciphers operate with a **time-varying transformation** on **individual plaintext digits.**
- Pseudo-random function (PRF): it takes two inputs and produces one output

BLOCK Ciphers

- Attacks to evaluate at certain points and skip to decide if it is useful.
- DES key can be found in 3 hours at a cost of $5000
- In attacks other then search attacks the cost of wiring, memory banks is high.
- Block cipher is a permutation with one huge cycle. Pre computation reduces time.

Message Authentication Codes

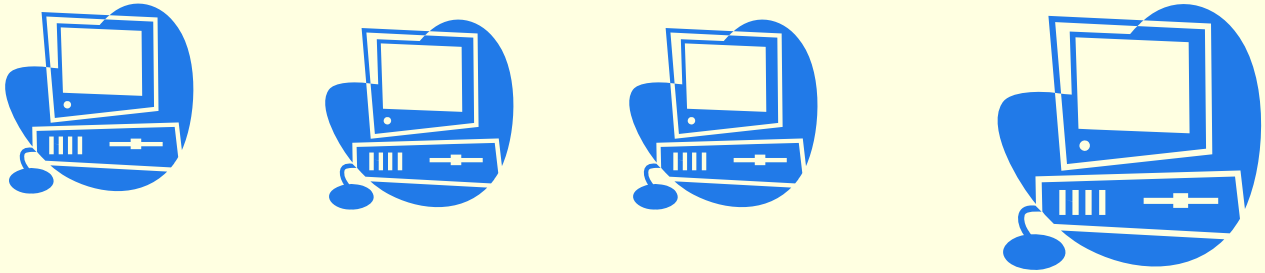
- MAC -Signing and verifying Algos create Message tags.
- HMAC creates encryption and MAC using a encryption and MAC Key. HMAC also breaks a large message into small blocks.

DES & AES

- Secret Key Cryptography (SK): Uses a single key for both encryption and decryption (DES, AES)
- Banking, messaging, transmission of secure data use DES/AES for encryption, general security, interoperability, authentication etc
- DES is a block cipher; it encrypts data in 64-bit blocks. A 64-bit block of plaintext goes in one end of the algorithm and a 64-bit block of ciphertext comes out the other end. DES is generally Hardware based.
- The key length is 56 bits. A handful of numbers are considered weak keys, but they can easily be avoided. All security rests within the key.
- At its simplest level, the algorithm is nothing more than a combination of the two basic techniques of encryption: confusion and diffusion. The fundamental building block of DES is a single combination of these techniques (a substitution followed by a permutation) on the text, based on the key. This is known as a round. DES has 16 rounds; it applies the same combination of techniques on the plaintext block 16 times.
- AES is another Cryptography standard basically successor to DES. AES is a block cipher; it encrypts data in 128-bit blocks instead of 64 for DES.
- Decryption in AES is **reversible** whereas in DES they **are invertible**.
- It follows three iterations XOR, substitution and permutation.
- AES has been incorporated in microprocessors as hardware programmable which results in an increase of speed. .
- Complexity of AES can be understood by the fact AES is a 3000 equation process.

Encrypting Credit Card Data
End to end encryption

POS



Pos terminal-processor #1-processor #2-processor #3-Acquiring bank

- Encrypted credit card should look like a credit card number
- Intermediate processors expect to see a credit card number

Disk Encryption

- Sectors on disk are fixed size (32k-48K)
- ENCRYPTION should not expand the plain text as no scope of it.
- If two sectors have the same plain text the cipher text will leak information about the key. So, every sector has to be encrypted with a different key for security.
- Common criteria is working on full Disk encryption and they have published a draft copy of the document on their web site.

Crypto for File Integrity, Downloading programs

- Secure Module (SM) generates Key from password – Key generates hash value for each file - stores it in a read only space of PC – virus infects file – boot next time – Hash value compared if yes go ahead otherwise restore.
- Secure Module (SM) generates Key from password – Key generates hash value for each file - stores it in a secure read only space of server – user downloads program calculates hash value for authenticity.
- One of the applications of File Integrity is fast booting by creating a certificate.

Some Issues

- Real world lightweight implementations.
- Exploits in the encrypted communication protocols.
- Assumptions on bad randomness.
- Key management (key distribution)
- Risk analysis frameworks for cryptographic systems

Crypto & Privacy

- one basic principle: the need to strike a balance between privacy and national security interests.
- A privacy system prevents the extraction of information by unauthorized parties from messages
- Put more positively, we routinely make trade-offs not just between privacy and security, but privacy and usability.
- Privacy has different meaning In US and Europe. IN US an individual has a right to protect personal information. In Europe the individual has a right to protect the information, created by him, for its life that is generated (history).

Crypto & Privacy

- The current standard definition of privacy for data analysis is differential privacy, which requires that the output distribution of the data analysis algorithm changes very little when a single individual's data is added or removed from the data set. Accurate differentially private algorithms for a wide variety of tasks have been developed, allowing for useful and private data analysis. This gives the same level of privacy protection for all individuals.
- Different levels of privacy protection to different individuals—intuitively, some individuals require more privacy than others,

Crypto & Law

Crypto being a new field laws have to be framed, certain countries legalise after the practice is accepted, some first pass the law and then practice it.

Crypto is a sensitive issue, national security of a nation depends on it. Many crypto algo developed by governments were kept secret and confidential. China has introduced its own satellite for secure communications. There are complicated laws governing export and use of crypto.

Some attacks

- Brute force
- Patterns
- Evasedroping : packet is redirected to another port
- Modifying : The packet’s checksum is modified by trial and error to find out the key.
- TCP/IP packages are submitted and by trial and error some knowledge about ciphertext.
- Ransomware

Indian Market

- E-commerce has a great demand for Authentication products based on crypto which could be achieved through Digital Signatures, Digital Certificates, tokens, passwords, QR codes, OTP generation, personal identification modules, etc.
- A great demand for crypto systems like EMV chip cards, Certificate Management, RFID Tags just to name a few also exsists.

Crypto Market (Ecommerce)

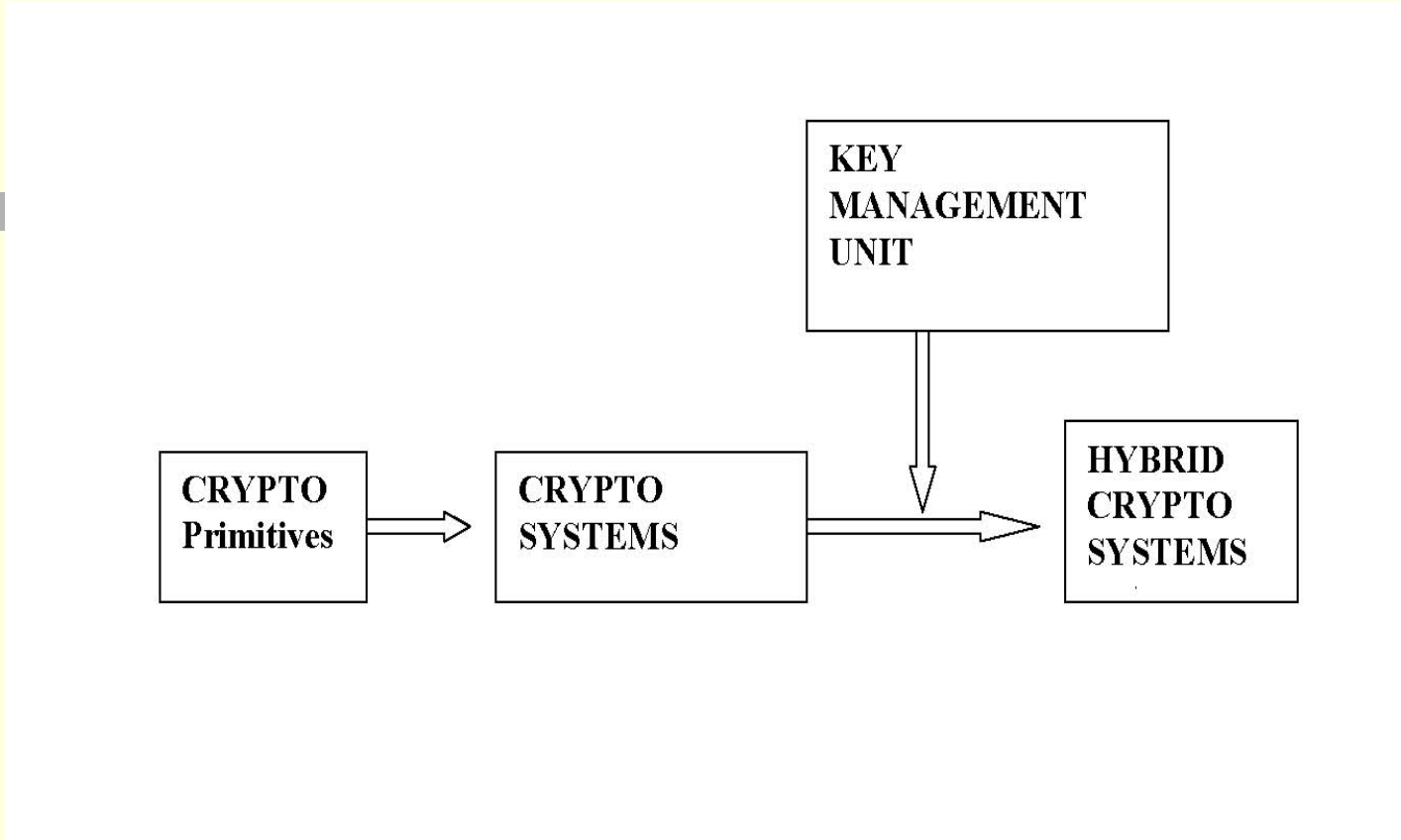
- Ecommerce is a fast growing segment of the Indian market. Ecommerce requires controls for access, transaction confidentiality, availability of the site, audit trails in which CRYPTO can play an important role.
- Many sites use legacy technology which has to be upgraded.
- Crypto can also upgrade security as a service to security products

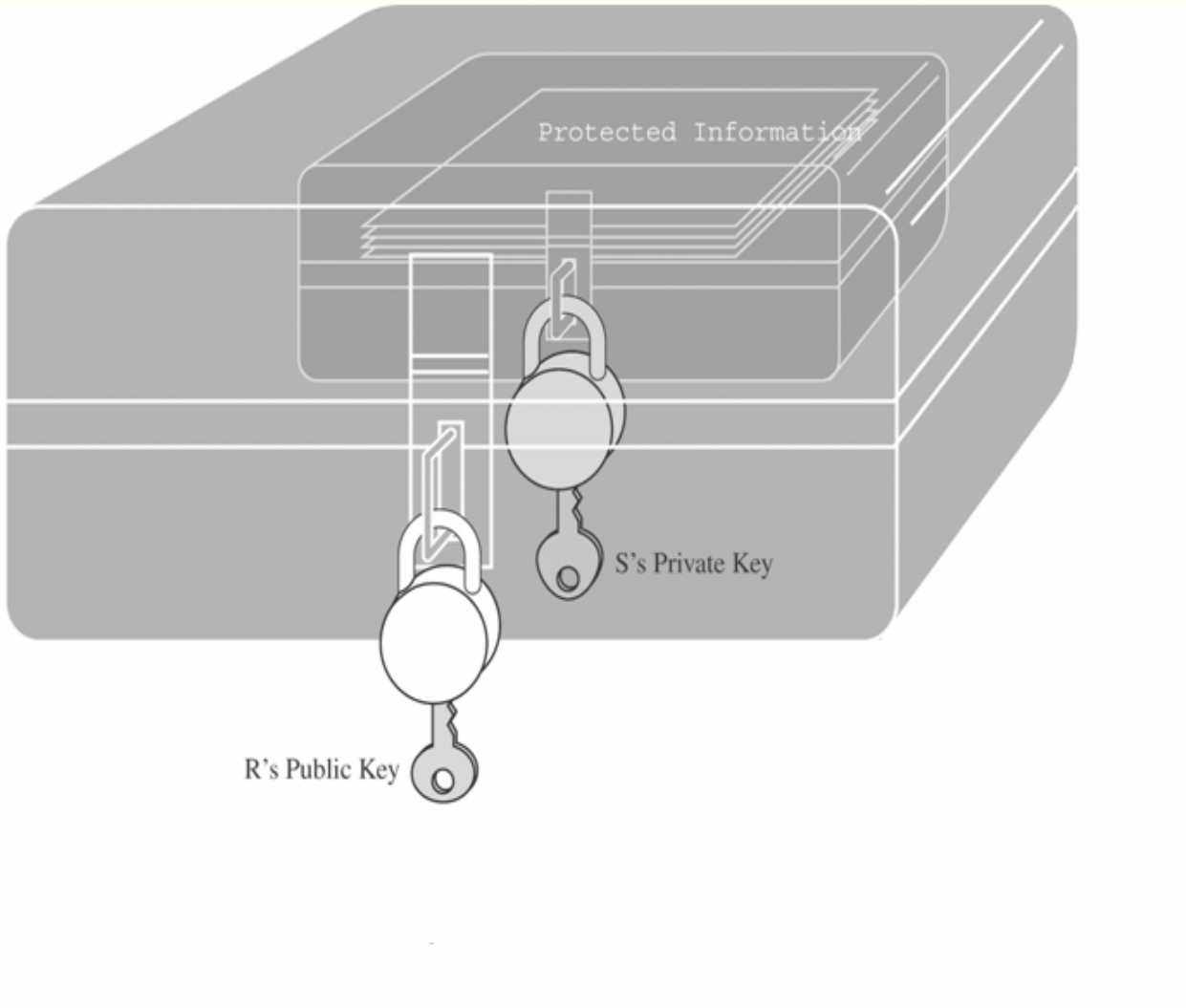
Security Controls in ECOMMERCE

- TLS/SSH (Communication)
- Two Factor Authentication (Access)
- Tokens (Access)
- Quad Codes (Access Control)
- File Integrity (Content)
- Mobile Security
- Key Management

Key Management

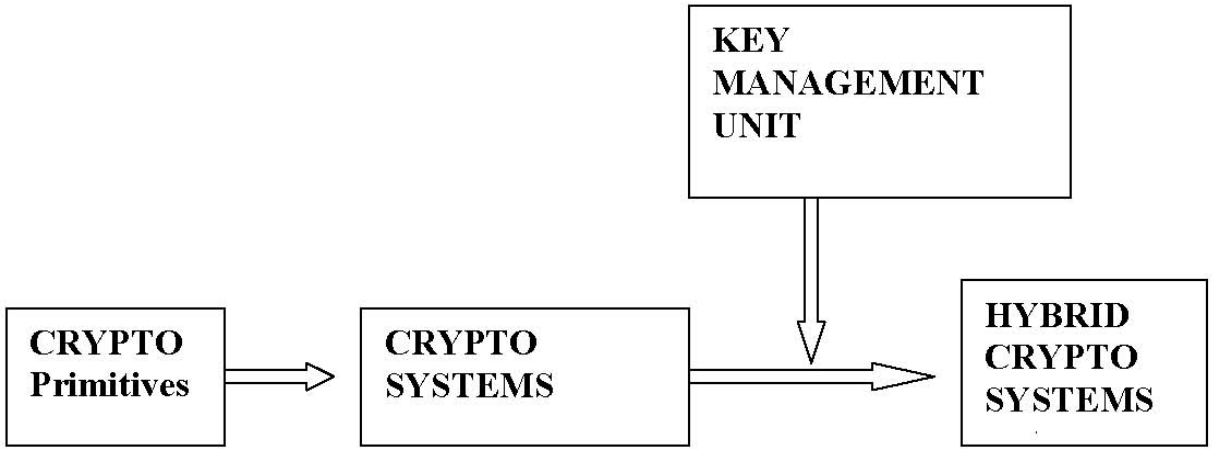
OBJECTIVE


KEY
MANAGEMENT
UNIT
CRYPTO
Primitives
CRYPTO
SYSTEMS
HYBRID
CRYPTO
SYSTEMS



The Idea Behind Key Exchange.

SUMMARY


KEY
MANAGEMENT
UNIT
CRYPTO
Primitives
CRYPTO
SYSTEMS
HYBRID
CRYPTO
SYSTEMS

CRYPTO RESEARCH SCENARIO

- A lot of research is going on to make crypto process more efficient by factors. The pace of research is such that VLSI chips based on FIPS are designed of the algorithm in a very short cycle.
- Secondly crypto products will enhance many applications like voting, auctioning, zero knowledge proof.

Crypto MacroView

PRORTOCOLS	DYNAMIC VALIDATION
Secret key Public/private key Hash	**Nonces** **PRG** **Timestamps** **Counters** **Padding**

By using the above protocols and validation in stepsone can build sophisticated hybrid crypto systems like One time keys-Blind keys-Group Keys-Broadcasting Signatures-Bearer certificates-Capability protection-certificate Generation to Retirement Certificates - –Manufacturing : input to output-Voting-Auctioning

Crypto New Applications

- Identification/Entity Authentication
- Access control
- Availability
- Auditing
- Physical security
- Anonymity

FUTURE APPLICATIONS

- Format Preserving Encryption,
- Lightweight implementations (RFID Tags)
- Digital Rights Management
- Key Management
- Hybrid Crypto products
- Computing (Searchable) encrypted data

Designers

- The designer (challenger) develops a system whereby the attacker has to do more work then the designer in terms of resources, time, energy and computational power. If designer uses one dimensional table the attacker has to use two dimensional table or an order higher.
- By using Secret key, Public/private key, Hash, Nonces, Random Generators, Timestamps, Counters padding, etc By using them insteps designer can develop sophisticated systems and also defend from attackers. (Digital signature is one)

User’s point of view

- Provide security
- When encrypting data the ciphertext and plaintext should be indistinguishable.
- Adv cannot learn anything of ‘message’,
- meaningful information of ‘m’
- Adv cannot learn any information of ‘m’
- Adv computational resources, capabilities and knowledge **a**reas **good as anybody else**.

OPEN SSL(Developers)

- An open source crypto library whereby one build crypto systems using various utilities :
- TLS/SSH
- Password Manager
- Private Certificate
- Digital Signatures
- Key and Certificate Management, Key Generation, Creating Certificate Signing Requests
- ZMAP – Open source **tool**

Auditing of Crypto Systems

- Policy
- Procedures
- Risk Analysis
- Risk Mitigation
- Vulnerabilities
- Conclusion

TESTING

- First test crypto like any other computer system and prove its correctness.
- BAN logic is the most widely used logic for analyzing authentication protocols. It assumes that authentication is a function of integrity and freshness, and uses logical rules to trace both of those attributes through the protocol.
- Formal verification

Suggested Norms

- Secret Key – 128 bit key is minimum
- Hash - !60 bits is minimum
- RSA – 2048 bits
- ECC – 128 bits

Verification

- Add high-level annotations
- Annotated code gets fed to verification tool
- Verification ensures that operation on limbs corresponds to high-level arithmetic
- Audits look at high-level annotations
- Even better: feed to even higher level verification
- Verify that the sequence of field operations accomplishes EC arithmetic

FIPS 140-2

- FIPS 140-2 standard examines 11 areas of a cryptographic module used by a device's security system, including physical security, cryptographic key management and design assurance. It is available in four qualitative levels offering increasing stages of security. **FIPS 140-2 Level 3** certifies the device is tamper-evident, employs the highest level of data encryption and thwarts attacks directed at the products' Critical Security Parameters. This rigorous testing and certification procedure offers reassurance for CIOs and IT Managers at every business.

Auditing

- Crypto with hash values can check integrity of data very fast and effectively this can be used to check configuiration files (just like anti virus) (standards have to be developed)
- Checking encrypted data is an open field but integrity of encrypted data can be checked.
- Searching of encrypted data

Conclusions

- Do not implement crypto on your own always depend on known systems.
- Cryptography field is evolving at a very fast rate and it will offer many solutions in many domains.
- Cryptography dynamic nature resists development of standards, only best practices are implemented.

ACRONYMS

Acronym	Meaning
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
DHKE	Diffie Hellman Key Exchange
DEK	Data Encryption Key
DES	Data Encryption Standard
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
HMAC	Keyed-Hash Message Authentication Code
IV	Initialization Vector
MAC	Message Authentication Code
MOD	Modular Arithmetic
NIST	National Institute of Standards and Technology
PRF	Pseudo Random functions
RSA	Private/Public Key Algorithm
SHA	Secure Hash Algorithm
XOR	Exclusive or

Contact details

- Hiten Mehta
- hitensm@gmail.com
- Mobile : 91-22-932-407-3221