**UNIT – II**

**BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY**

**PART-A**

1. **Define DES**

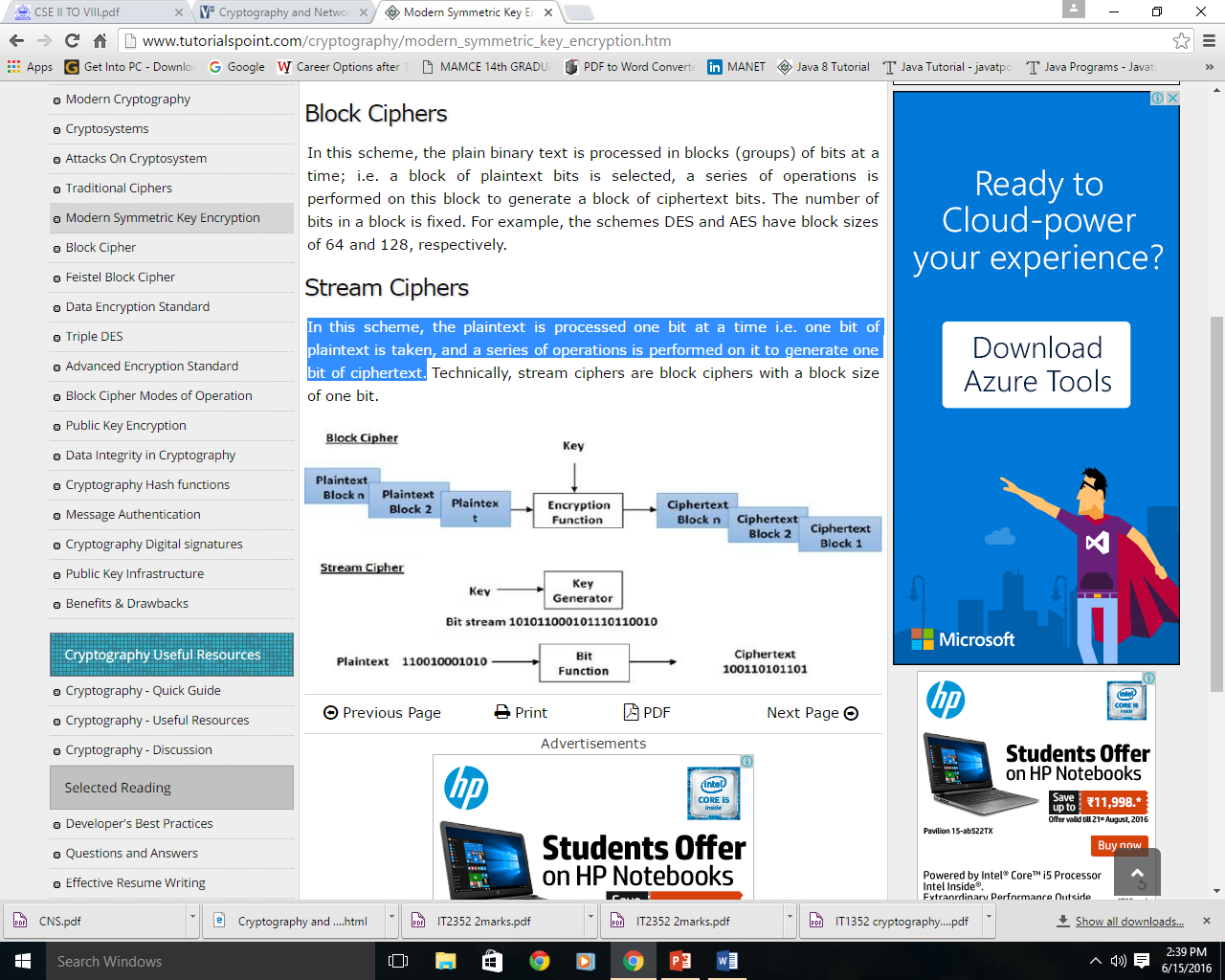
The Data Encryption Standard (DES) is a symmetric-key block cipher. DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit.

1. **What is a block cipher?** (APRIL/MAY 2015)

A block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size. The size of block is fixed in the given scheme.For example, the schemes DES and AES have block sizes of 64 and 128, respectively. 

1. **What is a stream cipher?** (APRIL/MAY 2015)

In this scheme, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of ciphertext.



1. **Compare stream cipher with block cipher with example. (APRIL/MAY 2015)**

* Stream cipher: Processes the input stream continuously and producing one element at a time. Example: caeser cipher.
* Block cipher: Processes the input one block of elements at a time producing an output block for each input block. Example: DES.

1. **What is meant by padding in Block Cipher?**

The process of adding bits to the last block are referred to as **padding**.Too much padding makes the system inefficient.

1. **Define Feistel Cipher.**

Feistel Cipher is not a specific scheme of block cipher. It is a design model from which many different block ciphers are derived. DES is just one example of a Feistel Cipher. A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.

1. **Differentiate public key and conventional encryption?(NOV/DEC 2011)**

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | **Conventional Encryption** | | |  | | --- | | **Public key Encryption** | |
| |  | | --- | | * The same algorithm with the same key is used for encryption and decryption. * The sender and receiver must share the algorithm and the key. * The key must be secret * It must be impossible or atleast impractial message if no other information is available * Knowledge of the algorithm plus samples of cipher text must insufficient to determine the key | | |  | | --- | | * One algorithm is used for encryption and decryption with a pair of keys, one for encryption and another for decryption. * the sender and receiver must each have one of the matched pair of keys. One of two keys must be kept Secret . * It must be impossible or to at least impractical to decipher a message if no other information is available. * Knowledge of the algorithm plus one of key plus samples of ciphertext must be insufficient to determine the other key. | |

1. **Mention the features of AES. (NOV/DEC 2011)**

The features of AES are as follows −

* Symmetric key symmetric block cipher
* 128-bit data, 128/192/256-bit keys
* Stronger and faster than Triple-DES
* Provide full specification and design details
* Software implementable in C and Java

1. **Mention some of the Block Cipher schemes.**

Digital Encryption Standard (DES)

Triple DES

Advanced Encryption Standard (AES)

1. **Mention some of the properties of public key encryption scheme.**

The most important properties of public key encryption scheme are −

* Different keys are used for encryption and decryption.
* Each receiver possesses a unique decryption key, generally referred to as his private key.
* Receiver needs to publish an encryption key, referred to as his public key.
* Encryption algorithm is complex enough to prohibit attacker from deducing the plaintext from the ciphertext and the encryption (public) key.

1. **Define ECC.**

Elliptic Curve Cryptography (ECC) is a term used to describe a suite of cryptographic tools and protocols whose security is based on special versions of the discrete logarithm problem.ECC is based on sets of numbers that are associated with mathematical objects called elliptic curves.

1. **Difference between RSA and ElGamal schemes.**

|  |  |
| --- | --- |
| **RSA** | **ElGamal** |
| It is more efficient for encryption. | It is more efficient for decryption. |
| It is less efficient for decryption. | It is more efficient for decryption. |
| For a particular security level, lengthy keys are required in RSA. | For the same level of security, very short keys are required. |
| It is widely accepted and used. | It is new and not very popular in market. |

1. **Define Blow Fish algorithm.**

Blowfish is an [encryption](http://searchsecurity.techtarget.com/definition/encryption) [algorithm](http://whatis.techtarget.com/definition/algorithm) that can be used as a replacement for the [DES](http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard) or[IDEA](http://searchsecurity.techtarget.com/definition/International-Data-Encryption-Algorithm) algorithms. It is a symmetric [block cipher](http://searchsecurity.techtarget.com/definition/block-cipher) that uses a variable-length [key](http://searchsecurity.techtarget.com/definition/key), from 32 bits to 448 bits, making it useful for both domestic and exportable use.

1. **Explain RC5 algorithm.**

The RC5 encryption algorithm is a fast, symmetric block cipher suitable for hardware or software implementations. A novel feature of RC5 is the heavy use of data-dependent rotations. RC5 has a variable-length secret key, providing flexibility in its security level.

1. **Mention the block cipher modes of operation.**

## Electronic Code Book (ECB) Mode

## Cipher Block Chaining (CBC) Mode

## Cipher Feedback (CFB) Mode

## Output Feedback (OFB) Mode

## Counter (CTR) Mode

1. **Why is AES preferable to triple-DES?**Primarily the larger block size (128) which makes suspected text cryptanalysis much more difficult.  Key length for triple-DES is actually larger than for AES.
2. **What is the purpose of the S-boxes in DES? (NOV/DEC 2011)**

In cryptography, an S-Box (Substitution-box) is a basic component of symmetric key algorithms which performs substitution. The S-boxes are the nonlinear part of DES that makes it difficult to break the algorithm and secure against linear and differential cryptanalysis. The s-boxes provide the "confusion" of data and key values.

1. **Mention the issues addressed by public key cryptography?**

Public key Cryptography is developed to address two key issues:

* **key distribution** – how to have secure communications in general without having to trust a KDC with your key
* **digital signatures** – how to verify a message comes intact from the claimed sender

1. **Perform encryption and decryption using the RSA algorithm, for the following:**

p = 3; q = 11, e = 7; M = 5

n = p x q = 3 x 11 = 33

ϕ(n) = (p-1) x (q-1) = 2 x 10 = 20

gcd(ϕ(n), e) = gcd(20, 7) = 1

∵ d ≡ e-1(mod ϕ(n))

d x e mod ϕ(n) = 1

7d mod 20 = 1

∴ d = 3

So: Public Key pu = {e, n} = {7, 33}

Private Key pr = {d, n} = {3, 33}

Encryption:

C = Me mod n = 57 mod 33 = 14

Decryption:

M = Cd mod n = 143 mod 33 = 5

1. **Define miller-rabin algorithm?**

* The [Miller–Rabin primality test](http://en.wikipedia.org/wiki/Miller%E2%80%93Rabin_primality_test) or Rabin–Miller primality test is a primality test: an algorithm which determines whether a given number is prime or not.
* The algorithm, as modified by [Michael O. Rabin](http://en.wikipedia.org/wiki/Michael_O._Rabin) to avoid the [generalized Riemann hypothesis](http://en.wikipedia.org/wiki/generalized_Riemann_hypothesis), is a probabilistic algorithm.

1. **What is triple encryption?**With triple encryption, a plaintext block is encrypted by passing it through an encryption algorithm; the result is then passed through the same encryption algorithm again; the result of the second encryption is passed through the same encryption algorithm a third time. Typically, the second stage uses the decryption algorithm rather than the encryption algorithm.
2. **If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate?**Nine plaintext characters are affected. The plaintext character corresponding to the cipher text character is obviously altered. In addition, the altered cipher text character enters the shift register and is not removed until the next eight characters are processed.
3. **Why is the middle portion of 3DES a decryption rather than an encryption?**There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES by repeating the key.
4. **Mention the advantages of ECB mode.(MAY/JUNE 2013)**

**Advantages**

This mode has two obvious advantages. First, it is simple. Second, transmission error is not propagated from one block to the other.

**Disadvantages**

This mode has some security problems. First, patterns at theblock level are preserved.

Second, block independency creates opportunitiesfor Eve to substitutes somecipher

blocks with some cipher blocks of her own.

1. **Mention some of the techniques of attacking RSA.**

### Searching the Message Space

### Cycle Attack

### Common Modulus

### Faulty Encryption

### Low Exponent

### Factoring the Public Key

**PART-B**

1. Explain data encryption standard in detail?(APRIL/MAY 2015)( MAY/JUNE 2013) MAY/JUNE 2014)(NOV/DEC 2012)
2. Explain the RSA algorithm in detail. For the given values, trace the sequence of calculations in RSA, p=7,q=13,e=5 and M=10. (APRIL/MAY 2015)
3. Explain about the single round of DES algorithm. (APRIL/MAY 2011)
4. Describe key discarding process of DES. (APRIL/MAY 2011)
5. Explain RSA method in detail. (APRIL/MAY 2011)( MAY/JUNE 2013) MAY/JUNE 2014) (NOV/DEC 2011) (NOV/DEC 2012) (NOV/DEC 2013)
6. Explain about triple DES with an example?(MAY/JUNE 2012)(NOV/DEC 2013)
7. Explain about Diffie Hellman key exchange algorithm with one suitable example. MAY/JUNE 2013) (MAY/JUNE 2014) (NOV/DEC 2012)
8. Demonstrate encryption and decryption for the RSA algorithm parameters p=3, q=11, e=7, d=? , M=5. (MAY/JUNE 2014)
9. Users A and B use the Diffie Hellman Key exchange technique with a common prime q=71 and a primitive root α=7. If user A has private key XA=5, what is A’s public key YA? (MAY/JUNE 2014)
10. Explain the Key Generation, Encryption and Decryption of SDES algorithm in detail?(NOV/DEC 2011)
11. Describe the mathematical foundations of RSA algorithm. Perform encryption and decryption for the following p=17,q=7,e=5,n=119,message=”6”.Use Extended Euclid’s algorithm to find the private key.(NOV/DEC 2014)
12. Consider a Diffie-Hellman scheme with a common prime q=353 and a primitive root α=3. Users A and B have private keys XA=17,XB=21 respectively. what is the shared secret key K1 and K2? (NOV/DEC 2014)