Date

Expt. No. Page No.

#11:- Digital Signature :- imp. app. similar to msg authentication app. is ↑. same operation like MAC, but in digital Signature hash value of msg is encrypted with users private key. anyone with private key can access.

- Hash functions are create a one-way password file, use for intrusion Pseudo random Number generater (PRNG). simplest hash func. bit-by-bit exclusive-OR (XOR) of every block.
- Brute-Force-Attack :- 2 attacks on hash func. Brute-force attacks and cryptanalysis. B-F-A doesn't depend upon on algo but depends on length of bit. of a hash value. but cryptanalysis is vice versa, it attack by taking the weakness of an algorithm. takes a value (y) and tries it at random till it reach collision.

SHA :- secure hash algo :- widely used, imp. and good hash algo, developed by NIST in 1993. new version is SHA-0 then SHA-1 SHA-192 Logic : takes input msg with max length 2^{128} bits and produce output 512-bit msg.

SHA-3 :- SHA-1 hasn't been broken, it is called insecure because its similar to SHA-0 and it can be insecure by today's calculation NIST announced competition in 2007, to produce next generation. called SHA-3 was announced in 2012 was published in 2015. SHA-3 intended to complement SHA-2 as approved standard for wide range app.

- Sponge Construction : has same structure as other hash func", takes input msg, partions it into fixed-size finally producing output block.
- Simple padding :- denoted by pad10*. appends a single bit 1 followed by min. no. of bits 0 such that length of result is a multiple of block length.
- Multirate padding :- denoted by pad 10*1. appends a single bit 1 followed by min. no of bit 0 followed by single bit 1 such that length is multiple of block length.

Symmetric:-

Asymmetric:

Data integrity: protects block data from alteration like msg.

Authentication protocol:-

protection

computer security:- ~~affords~~ provided to automated information system in order to attain protection ~~of~~ through confidentiality, availibility, integrity for information system resource.

- Data confidentiality → Assures priv. info is secured.
- privacy
- system work properly & No service denied user
- Data integrity
- system integrity → system perform function free from unauthorized manipulation of system.

Confidentiality:- preserve restriction on info.

integrity:- Guard against improper info modification loss = unauthorized modification

Accountability:- generates request for action to be traced, Trace security.

Authenticity:- verifies users and sources.

Euclidean Algo: Basic of number theory, It determines GCD Greatest common Divisor. of two pt integers.

Millar-Rabin Algo: shown as [KNUT98]:— given no.(n) which is not integer the prob probability of it to be inclusive is 1/4. $1 < a < n-1$.

Deterministic Primality Algo:. till 2002 no method to prove it. by a large number is in poly AKS developed ↑ to check determine large number are prime no. or not.

Distribution of Prime = $\Omega(1/\ln(n))$ $n = 2^{200}$ => $0.5 \ln n = (2^{200})$.

Chinese Remainder Theorem (CRT) :- very useful, number theory, it is possible to reconstruct integer in certain range.

Binary operation mod:. a & n is integer, then we say a mod n ~~to be~~ remainder, when a divided by n. 'n' is modulus remainder is residue.

Stream cipher:- encrypts a digital data stream one bit/byte at a time. Ex:- Vernam Cipher if key is random then its breakable, key should be through secure channel.

Block cipher:- blocks of plaintext is treated as a whole and used to produce cipher text block of equal length.

FEISTEL Cipher:- [FEIS73] approximates block cipher by utilizing concept of product cipher final result is cryptographically stronger than any other component cipher.

- Hash need ed for security app
- Hash function determines if data has changed.
- Hash looks at range of app in which it is employed

Msg-Authentication:- Is Mechanism/ service to verify integrity (send/receiving

Digital signature is same as MAC, but in this hash value of msg is encrypted
developed on public-key cryptography, provides set of security capabilities
that is difficult to implement other way.