P 🡪 D**A** 🡪 D**A** (P) 🡪 EA 🡪 EA D**A** (P) = P : Non-repudiation

P 🡪 E**B** 🡪 E**B** (P) 🡪 DB 🡪 DB E**B** (P) = P :

Confidentiality

P 🡪 D**A** 🡪 D**A** (P) 🡪 EB 🡪 EBD**A** (P) 🡪 DB 🡪 DB EBD**A**(P)

DA(P)🡪 EA 🡪 EADA(P) = P

P

MD(P) : Fingerprint of msg (P)

P ----hash function -- > MD5

P’ ----cannot give 🡪 MD5 that is equal to MD5 of P

MD5 -- not possible🡪 P

MD-P 🡪 DA 🡪 DA (MD-P)

Party 1 Party 2

CT1, MD1 CT2, MD2

P, MD(P)

Compute MD(P)

Verify if MD(P) == MD(P)

EBDB

RSA

1. Choose (**large**) 2 prime nos. (1024 bits)
2. product of them, say n = p \* q
3. z = (p – 1) \* (q – 1)
4. Choose a number ~~d~~ e such that it is coprime to z
5. Choose e such that e \* d = 1 (mod z), or (e \* d) % z = 1
6. Public key: (e, n) ; Private key: (d, n)
7. C = Pe(mod n)
8. P = Cd (mod n)

Hello

7 4 11 11 14

0111 0010 1011 1011 1110

m: 28 < n

0 \le m < n

1. Take p = 3 and q = 11
2. n = 33
3. z = (3 – 1) \* (11 – 1) = 20
4. Let d = 3
5. (e \* 3)%20 = 1 => e = 7
6. m = 2 ; C = ? 27 (mod 33) = 128 mod 33 = 29
7. P = 293(mod 33) = 2

((Apublic\_key )TA\_pvt\_key)TA\_public\_key