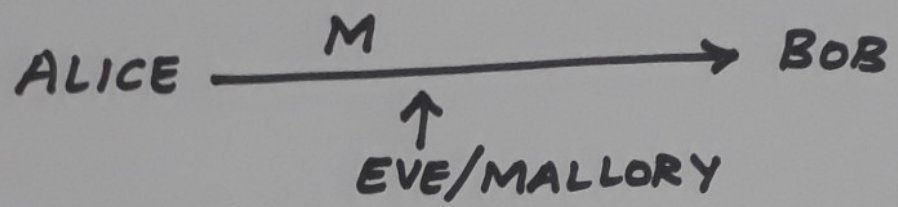
A LIGHTNING PRIMER ON CRYPTO.

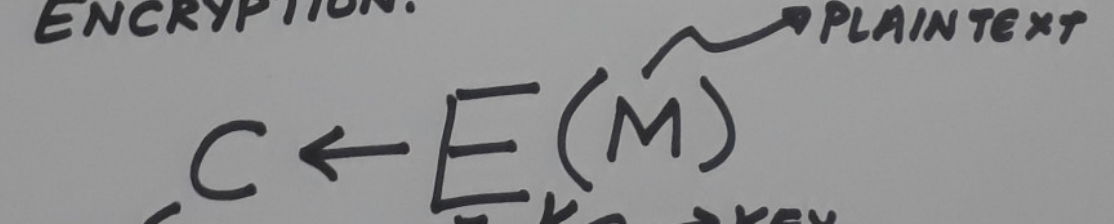
ACTORS:

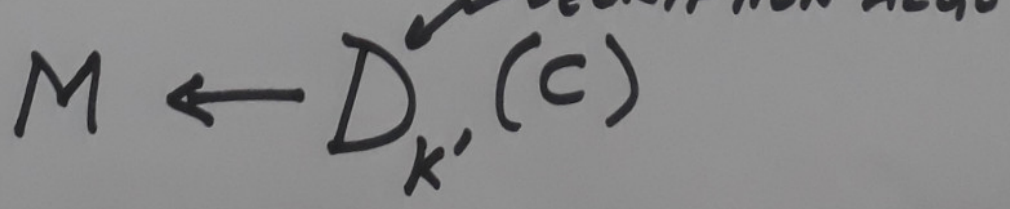


CONFIDENTIALITY OF M?
INTEGRITY OF M?
SENDER AUTHENTICATION?
NON-REPUDIATION (ABILITY TO PROVE MESSAGE WAS SENT BY SOMEONE).

HOW?.

ENCRYPTION.





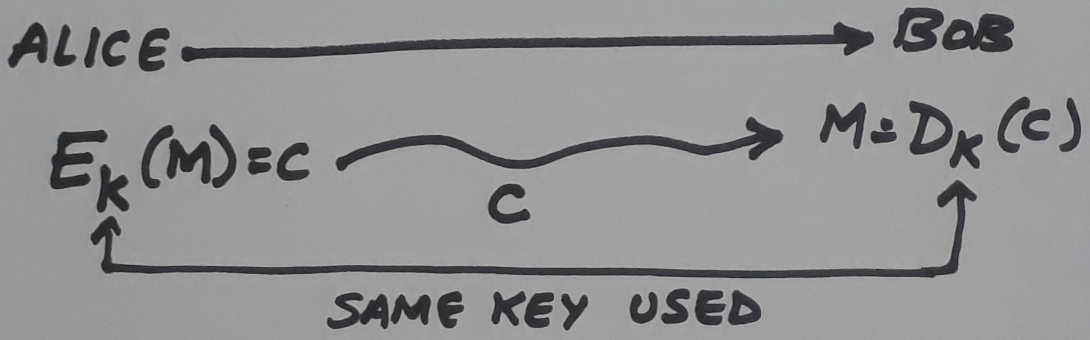
VARIOUS TYPES OF ALGOS

- STREAM CIPHERS (e.g. RC4)
- BLOCK CIPHERS (e.g. DES, AES, RSA)

WE WILL TALK ABOUT BLOCK CIPHERS.

TWO TYPES EVEN THERE:

- SYMMETRIC-KEY CIPHERS



EXAMPLE: AES.

GENERALLY FOLLOW A STRUCTURE CALLED A FIESTEL CIPHER —

SEE HANDOUT.

CREATED VIA WORLD-WIDE COMPETITIONS.

KEY SIZES ~ 512-2048 bits.

PROBLEM WITH SYMMETRIC-KEY CIPHERS

→ How Do ALICE/BOB SHARE k in the FIRST PLACE?! —— [Q KEY]

- PUBLIC-KEY CRYPTO:

BOTH ALICE & BOB EACH HAVE SOME PUBLIC & SOME PRIVATE (i.e KNOWN ONLY TO THEM) PARAMS.

MOST BASIC EXAMPLE:

DIFFIE-HELLMAN KEY EXCHANGE.

SOLVES THE [Q KEY] PROBLEM ABOVE.

- BASED ON HARDNESS OF DISCRETE LOG.
  - SUPPOSE $A \equiv B^x \pmod{p}$

THEN x is called DISCRETE LOG OF A TO BASE-B, mod p.

GIVEN A, B, P, all large enough, computationally hard to find x.

DIFFIE-HELLMAN KEY EXCHANGE

ALICE : (g, p) : PUBLIC a : PRIVATE

BOB : (g, p) : PUBLIC b : PRIVATE

① ALICE $\xrightarrow{(g^a) \bmod p}$ BOB.

② ALICE $\xleftarrow{(g^b) \bmod p}$ BOB

③ ALICE: $(g^b)^a \bmod p = g^{ab} \bmod p$

④ BOB: $(g^a)^b \bmod p = g^{ab} \bmod p$.

$g^{ab} \bmod p$ is a SHARED SECRET.

SECURITY ARGUMENT:

→ given $g^a \pmod p$, g, p, BOB cannot infer a unless Discrete log is "easy".

RSA: MAJOR PUBLIC-KEY ALGO:

ALICE: PUB_A, $PRIV_A$

BOB: PUB_B, $PRIV_B$

TO SEND A MESSAGE FROM ALICE TO BOB:

ALICE $\xrightarrow{E_{PUB_B}(M)}$ BOB

BOB DECRYPTS:

$$D_{PRIV_B}(E_{PUB_B}(M))$$

AND THIS YIELDS M.

NO OTHER ENTITY CAN DECRYPT AS $PRIV_B$ IS PRIVATE TO BOB.

LATER WE WILL ALSO STUDY RSA-BASED DIGITAL SIGNATURES

RSA IS A TOUR-DE-FORCE IN APPLYING ELEMENTARY NUMBER THEORY.

→ (FERMAT'S LITTLE THEOREM)

• LEMMA: LET p be a prime and $\gcd(a, p) = 1$. THEN, $a^{p-1} \equiv 1 \bmod p$

PROOF:

CONSIDER THE NUMBERS $x_1, x_2 \ldots x_{p-1}$

$a \pmod p$, $2a \pmod p$, $\ldots$

$(p-1)a \pmod p$

NOW, $x_1, x_2 \ldots, x_{p-1} \in \{1, 2, 3, \ldots, p-1\}$

CLAIM: THE SET $S = \{x_1, x_2, \ldots, x_{p-1}\}$

is in fact $\{1, 2, 3, \ldots p-1\}$

WHY? SUPPOSE NOT. THEN SOME

$x_i = x_j$, ie ~~$a_i = a_j \bmod p$~~

$ia \equiv ja \bmod p$

$i, j < p$, and a, p are coprime.

SO,

$$\prod x_i = (p-1)! \equiv (p-1)!\, a^{p-1} \pmod p$$

$\gcd((p-1)!, p) = 1$, SO $1 \equiv a^{p-1} \pmod p$

- $\phi(n)$: TOTIENT FUNCTION
  - → THE NUMBER OF INTEGERS $< n$ THAT HAVE $\gcd(\cdot, n) = 1$
- $\phi(\text{prime}) = (\text{prime} - 1)$
- $\phi(p \times q) = (p-1)(q-1)$
- LEMMA: ~~LET p be a pr~~

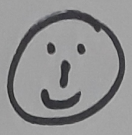
  LET n be an integer and a another integer so that $\gcd(a, n) = 1$

  THEN $a^{\phi(n)} \equiv 1 \pmod{n}$

PROOF: EXERCISE 

(similar in structure to proof of FERMAT'S LITTLE THEOREM)

COROLLARY: Let $n = p \times q$, a product of 2 primes. Let $M < n$. Then, for all integers x $M^{x \cdot \phi(n)+1} \equiv M \pmod{n}$

PROOF: Exercise! 

Here is how RSA WORKS.

- Alice chooses 2 primes p, q
- She computes $\phi(p \times q) = (p-1) \cdot (q-1)$
- n is used to denote $p \times q$
- she chooses an integer $e < n$
- she finds d such that $e \cdot d \equiv 1 \bmod \phi(n)$
- (e, n) is her public key
- (d, n) is her private key.

Factoring is computationally hard. An adversary who knows n cannot easily find $(p \& q)$. Thus given (e, n) adversary cannot find (d, n)

Say $Pub_A = (e_A, n_A)$, $Priv_A = (d_A, n_A)$

$Pub_B = (e_B, n_B)$, $Priv_B = (d_B, n_B)$

Recall that Alice, to send M confidentially to Bob does $E_{Pub_B}(M)$

$E_{Pub_B}(M)$ is implemented as

$$C = M^{e_B} \pmod{n_B}$$

M is broken into chunks (blocks) each less than n_B & each chunk is encrypted as above.

To decrypt, Bob does $D_{Priv_B}(C)$

This is implemented as

$$C^{d_B} \pmod{n_B}$$

Now,

$$C^{d_B} \pmod{n_B}$$

$$\equiv M^{e_B \cdot d_B} \pmod{n_B}$$

note that $e_B \cdot d_B \equiv 1 \bmod \phi(n_B)$

so $e_B \cdot d_B = x \cdot n_B + 1$

By the corollary theorem

$$\equiv M^{x n_B + 1} \pmod{n_B}$$

$$\equiv M \pmod{n_B}$$

M is processed in chunks each less than n_B.

Thus $M \pmod{n_B}$ is nothing but M.
