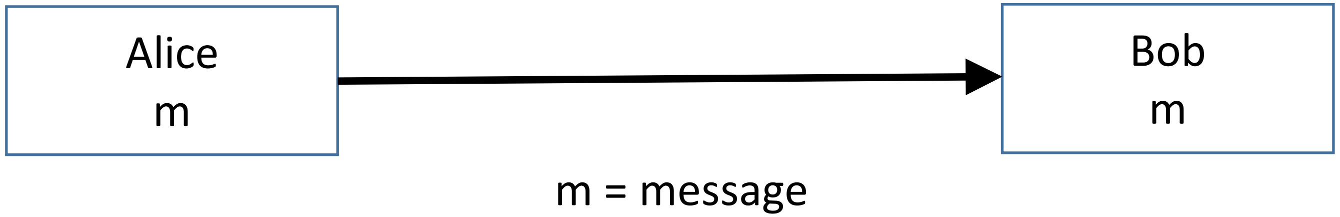
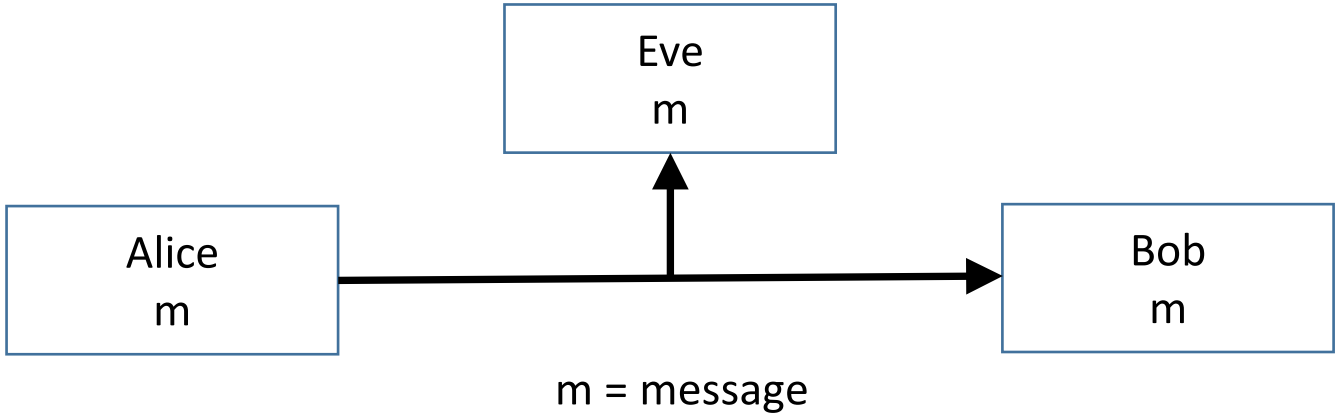
Class 2

Introduction to Cryptography

Alice transmit a message **m** Bob

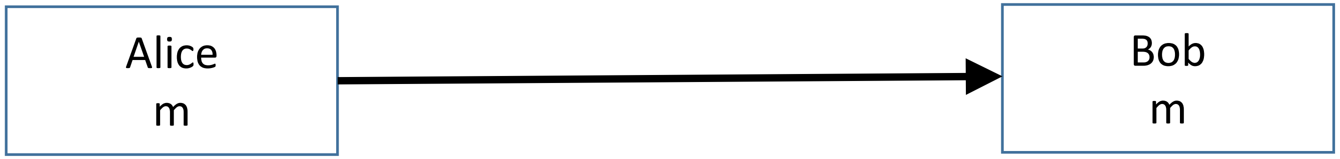


Eve is interested to: eavesdrop or change message



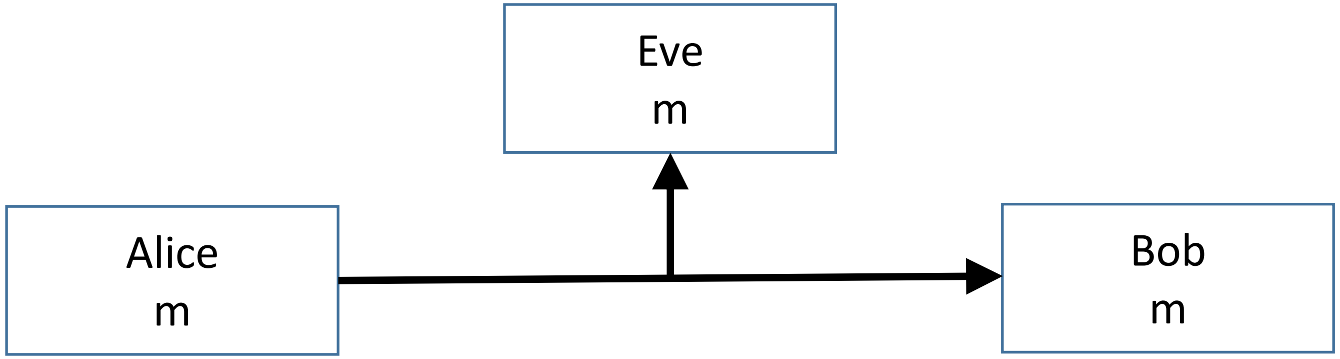
General model for communication

Alice transmits a message **m** Bob



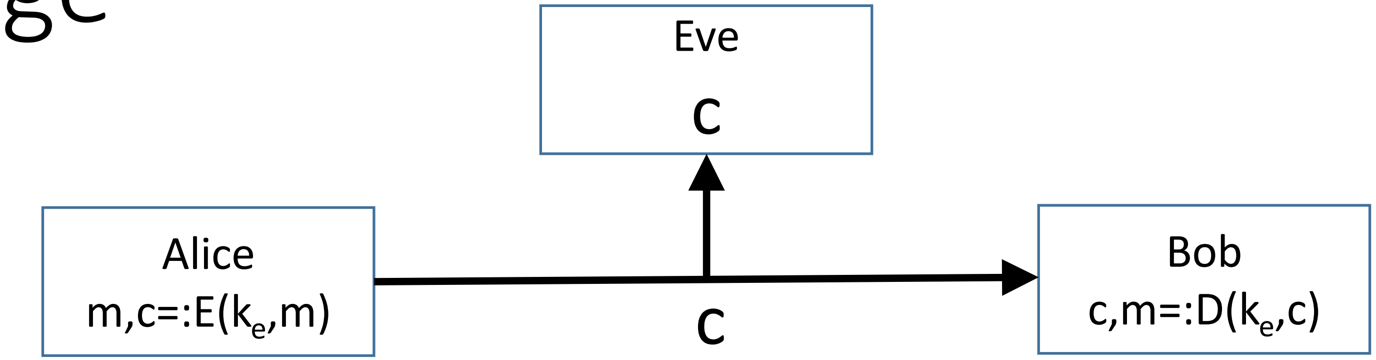
m = message

Eve is interested to EAVESDROP the message



m = message

Encryption: Preventing Eve to eavesdrop the message



K_e: Secret Key, the longer the key the highest the work factor. Shared by Alice and Bob.

m: A plaintext message.

E(K_e,m): Encryption function, a reliable one makes impossible to find the plaintext without knowing the key. Plaintext size and transmission time can only known to the attacker.

c: Ciphertext, Alice send it to Bob. Result of the encryption.

D(K_e,c): Decryption function is used to obtain the message (m).

Encryption: Kerckhoffs’ Principle

Bob will need Decryption algorithm **D** and the Key $\mathbf{k_e}$ to find the plaintext **m**

$$m=:D(k_e,c)$$

Kerckhoffs' principle: the security of the encryption scheme must depend only on the secrecy of the key K_e, and not on the secrecy of the algorithm.

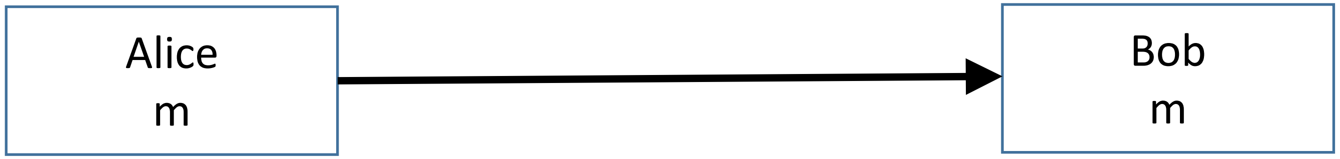
Implication :

If public, an encryption algorithm can be scrutinized to find failures/weaknesses prior implementation.

Hard to change, they are massively deployed via software and / or hardware

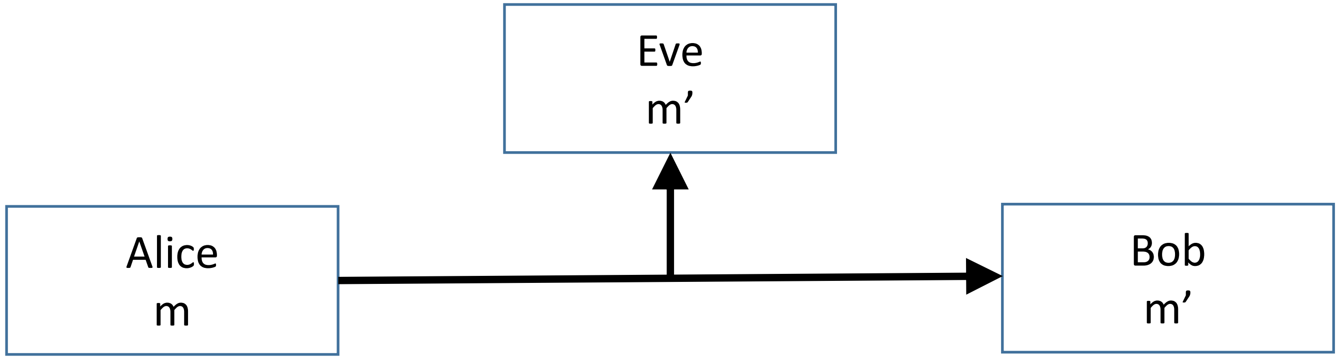
General model for communication

Alice transmit a message **m** Bob



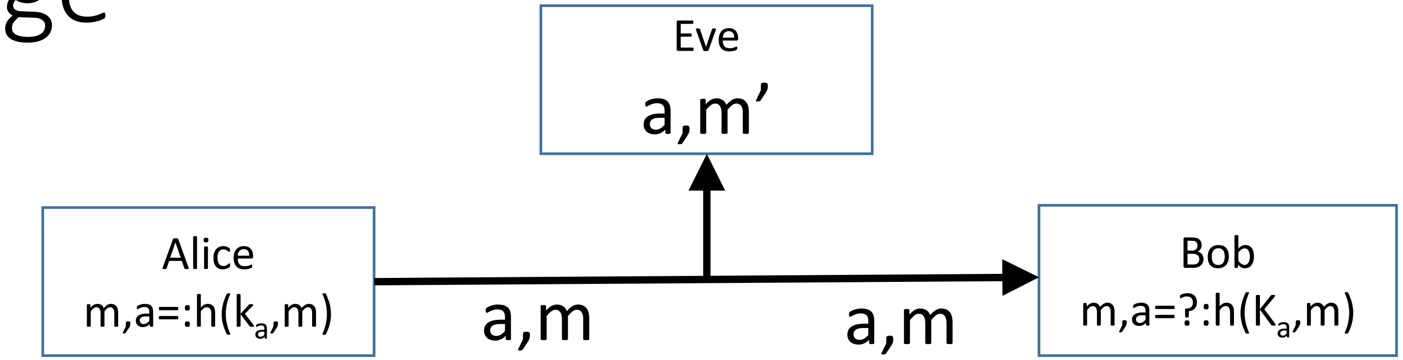
m = message

Eve is interested to **MODIFY** the message



m = message

Authentication: Preventing Eve to modify the message



k_a: authentication key.

m: plaintext message.

a: Message Authentication Code (MAC)

$h(k_e,m)$: h is the MAC function

Authentication

Eve can copy valid messages and replay them or intercept and delete them.

Authentication combined with a numbering scheme to number the messages sequentially.

Consider the message M={m_1,m_2,…,m_n} size n

Bob only accepts messages with:

- proper MAC
- Bob will discard new messages with previous accepted sequence number

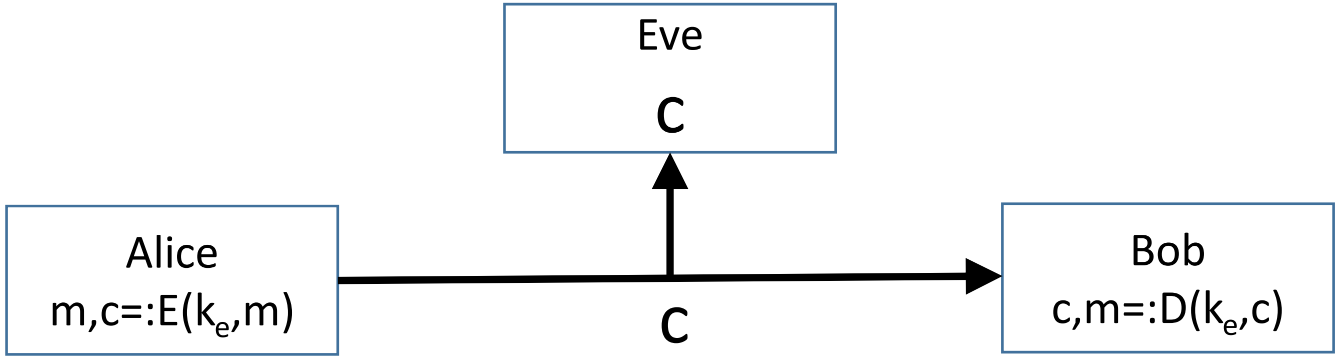
Worst case scenario Bob will get M’ with a size t, a subset of M where t <n

How Alice and Bob will handle deleted messages?

Authenticating a message doesn’t keep the message secret and encrypting a message does not prevent alteration of it contents.

Public key encryption

Bob and Alice use k_e how did they exchange it?

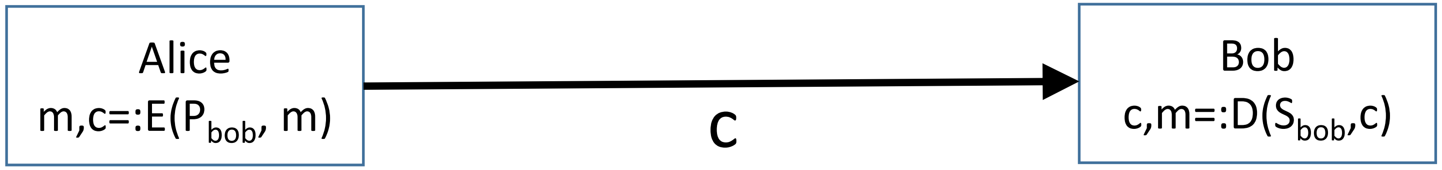


How about if Alice would like to communicate to other 10 people,
How many key exchanges would need to be done for a group of N people?

Total Key Exchanges = N(N-1)/2

Distribution of keys difficult challenge in cryptography.

Public Key Encryption



Alice

m,c=:E(P_{bob}, m)

c

Bob

c,m=:D(S_{bob},c)

Key pair generated by Bob, Public (P_{bob}) and Private (S_{bob}).

Alice uses Bob’s Public key to encrypt m, Bob decrypt the message using his Private or Secret Key.

Public key should not be able to be computed from private key.

Algorithm for encryption and decryption are related to obtain all possible messages m:

$$D(S_{bob}, E(P_{bob}, m)) = m$$

Public Key Encryption

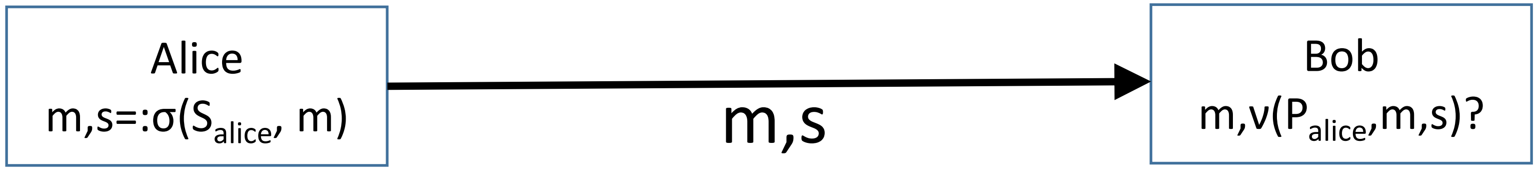
Bob and Alice can encrypt messages by using the public key component published in a system accessible for both or others.

Public key Encryption is also know as Asymmetric encryption.

Low performance compared to Symmetric encryption.

“The public-key algorithms are used to establish a secret key, which in turn is used to encrypt the actual data”

Digital Signatures



Alice

m,s=:$\sigma(S_{alice}, m)$

m,s

Bob

m,$v(P_{alice},m,s)$?

Alice generates a key pair (S_{Alice} , P_{Alice}) using a key generation algorithm.

Alice publishes Public Key (P_{alice})

Alice computes a signature ***s*** and sends it a long with the message m.

Bob use **v** a verification algorithm to check the validity of the received signature using Alice’s public key.

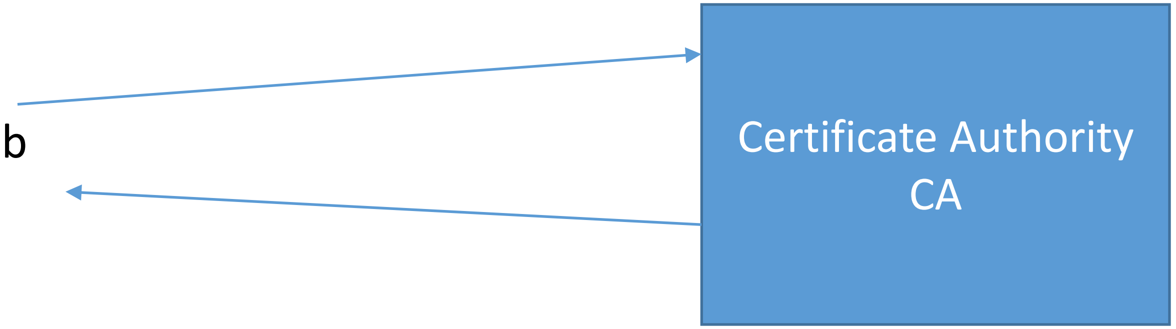
Digital Signatures

A third party tool used to compute (computer) the Digital Signature *S*

What if the computer is compromised?

Public Key Infrastructure

- Bob sends Public Key to CA P_{Bob}



- CA send back a Signed Public key encapsulated into a X509 Certificate: The CA will include expiration time, expedition time and the information identifying the CA among other information.

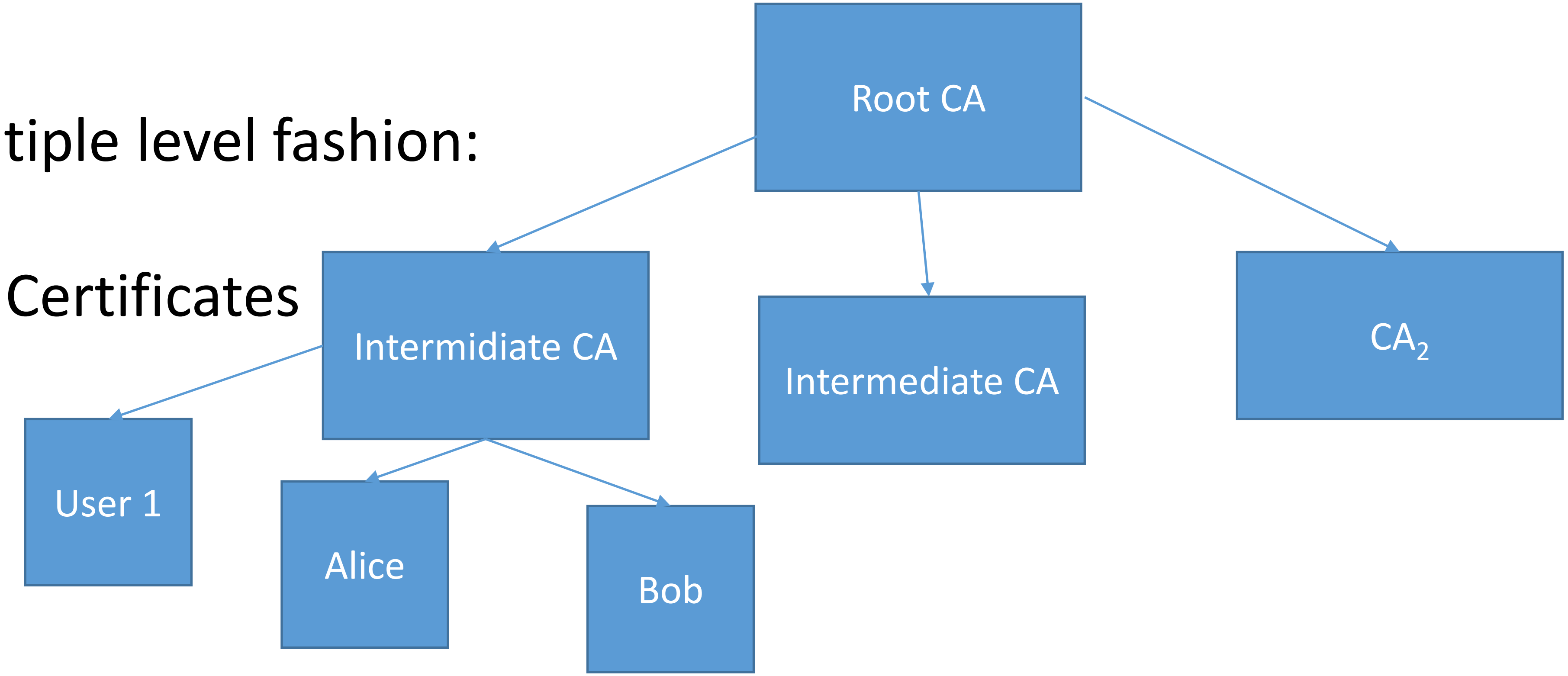
- Alice obtains (and verify) the CA Public Key from a Database or Bob can send it to her. She can verify Bob’s public key using the CA’s public key.

Public Key Infrastructure

In general, a user can be certified by the CA once and then by using the CA Public Key being validated by every user participating in the organization.

CA setup in a multiple level fashion:

Alice will check 2 Certificates to validate Bob



Public Key Infrastructure

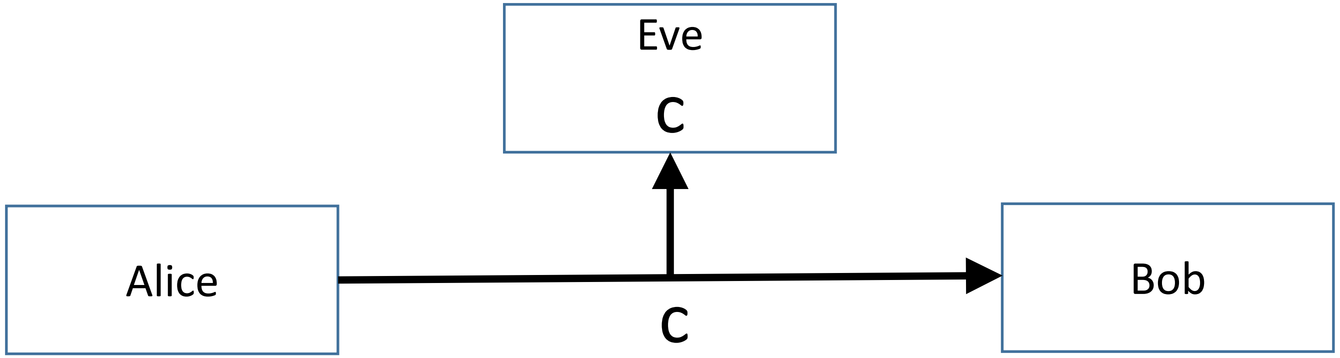
Possible PKI issues:

- Single point of failure, Private CA Key compromised or stolen.
- CA could issue a false certificate
- Trust, one CA for all?

Commercial CAs Verisign, DigiCert
Government DOEgrids
Academic/Research CERNCAs

Attacks
The Ciphertext-Only Model

The attacker tries to decrypt the message by only knowing the ciphertext.



Most difficult attack least amount of information used by the attacker.

Attacks: Known-Plaintext Model

The goal of this attack is to find the encryption key.

The attacker will know the plaintext (m) and the ciphertext (c).

The plaintext could be found in situations where predictable messages
are used:

Bob send an email to Alice, Alice‘s email client automaticaly replies that she is out on vacation. Similar ciphertext generated by Alice.

Attacker can send email to Alice, which generate similar type of reply.
Attacker knows the ciphertext and the message.

Attacks: Known-Plaintext Model

A predictable start and end of e-mails or IP datagrams header can lead to a plaintext/ciphertext matching.

The Chosen Plaintext model

Attacker decides plaintext and Cipher values (m,c). So:

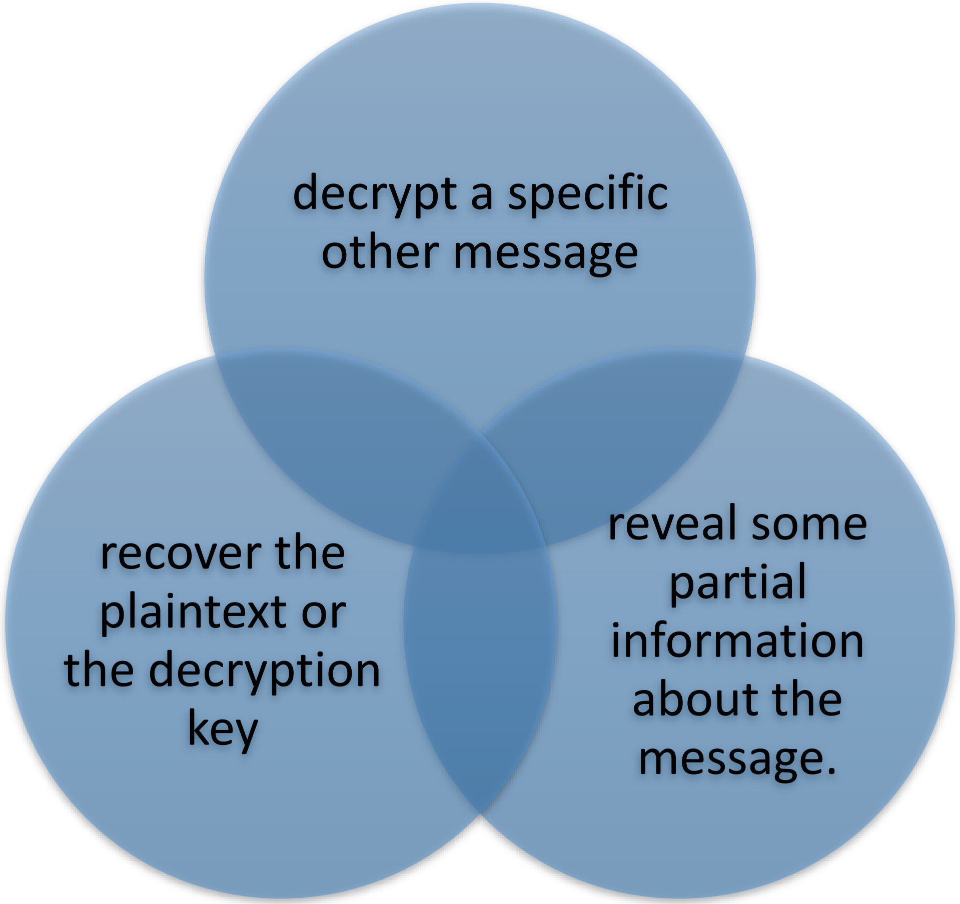
For plaintext → ciphertext

For ciphertext → plaintext

Main goal is to recover the key.

The Distinguishing attack goal

- Different attacks types and goals



decrypt a specific other message

recover the plaintext or the decryption key

reveal some partial information about the message.

The Distinguishing attack goal

“A distinguishing attack is any nontrivial method that detects a difference between the ideal encryption scheme and the actual one”

Other type of attacks

Besides attacking the encryption function the attacker can target the Authentication and Digital Signature cryptographic functions.

Information leakage or side-channel attacks; in addition to attach the encryption function sampling of the behavior of the encryption process, encryption speed and length.

Generic attacks techniques: Birthday attacks

Attack that depends on duplicated values, also called collisions.

Named after the Birthday Paradox

How many students will be needed in a class before the probability of having two people with the same birthday exceeds 0.5?

Number of pairs: $(23 \times 22)/2 = 253$

Probability of selecting a birthday: 1/365

In general if k is the number of inputs and N is the number of outputs there are $k(k - 1)/2$ input pairs each 1/N chance of being a pair of equal values

If $k(k - 1)/2 > N$, then likelyhood of getting a collision of 50% is $k > n^{1/2}$

So the chance of finding a collision is close to

$$k(k-1)/2*1/N$$

Generic attacks techniques: Birthdays attacks

For a n bit input we have $2^n = N$ possible values.

The number of elements required to have a collision is

$$N^{1/2}= k \text{ or } k=2^{n/2}$$

Known as *birthday bound*

Meet-in-the-Middle attacks

The attacker build a table size $2^{n/2}$ and actively create a MAC. Using this information eavesdrops the messages to try to find a match.

The message used could be a standard protocol call. i.e
“Ready to transmit data”

Overall if a key of n=64bits is used to authenticate a transaction,
In the standard case:

- A collision is expected to be encountered after 2^{32} key usages. Attacker will be waiting until this event is observed.

Using the Meet in the middle attack more flexible than Birthday attack

If there are N possible values .
Two sets of P and Q elements, a collision is expected when PQ/N -> 1

Meet-in-the-Middle attacks

If P and Q might be close to $N^{1/2}$ (Birthday bound).
In some situation is simpler to get elements for one of the sets, as long as PQ is close to N.

Say P is close to $N^{1/3}$ and Q is close to $N^{2/3}$ the attacker could make a list of 2^{40} possible MAC values for the first value and expect to get the first authentication key after listening to only 2^{24} transactions.

Security Level

How much work it takes to break a system?

If using an exhaustive search attack it tries all possible values.
Thus, if it takes 2^{256} steps to work, this corresponds to an exhaustive search for a 256 bit value.

Single step occurs when attacking an encryption function, computing a single encryption of a given message with a given key.
A single steps ---> single clock cycle.
A system needs today needs a 128 bits security level. A secure system should be designed to provide security for 50 years.