Latex Template

Raffaele Castagna

Academic Year 2025-2026

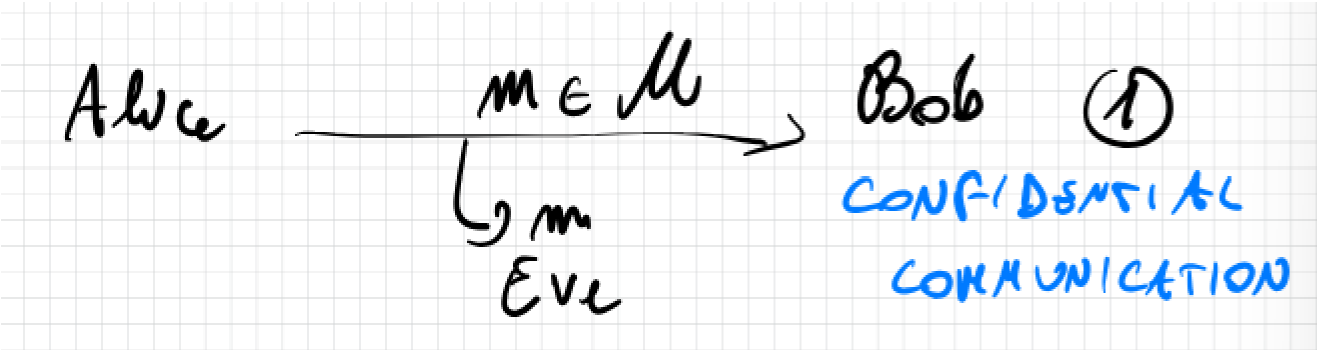
Contents

1 Intro to Cryptography

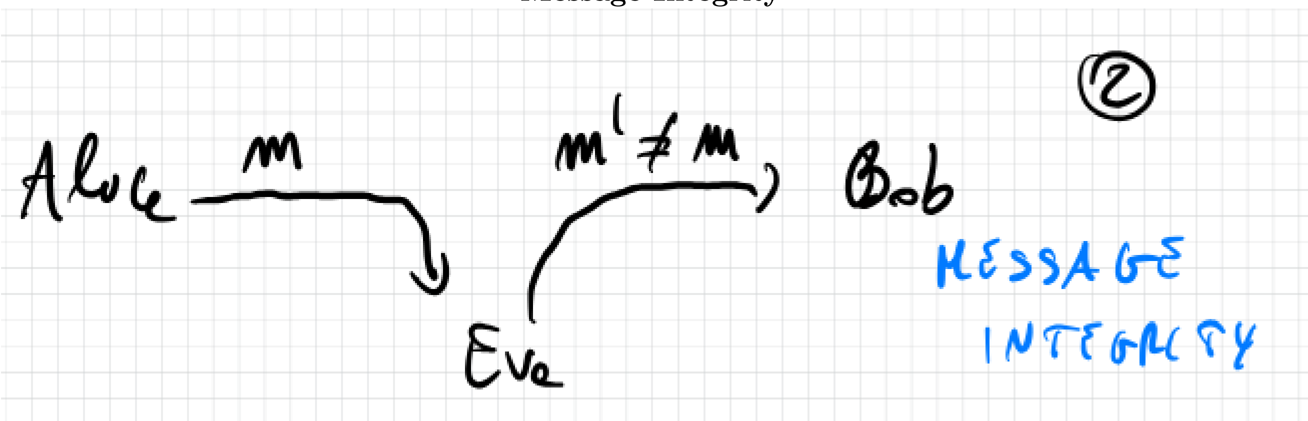
1.1 Secure Communication

We have multiple goals in cryptography, the most important ones being:

Confidential Integrity



Message Integrity



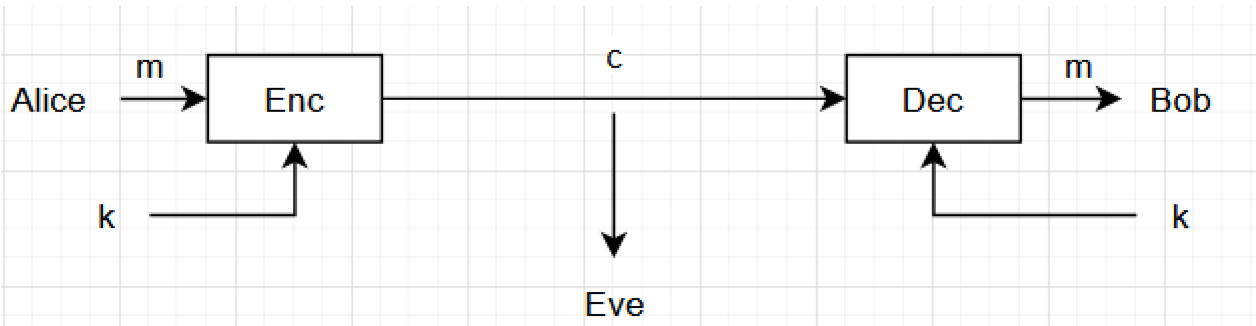
Basically we want our message to be both **confidential**, so no-one except the intended target sees it and we it to be unmodified, so that its **integrity** has not been compromised.

There are many different ways to do this, but in our case we only see two major ways:

- **Symmetric Cryptography**: Where Alice and Bob share a key $k \in \mathscr{K}$,the key is random and unknown to
- **Assymetric Cryptography**: Where Alice and Bob do not share a key, but they have each their own key pair (p_k, s_k) where p_k is the public key and s_k is the secret/private key

1.2 Unconditional Security

To achieve confidential communication, we use symmetric cryptography.



With $m \in \mathscr{M}, c \in \mathscr{C}, k \in \mathscr{K}$

In this case we have Alice sending a message m which is then encrypted utilizing a randomly generate key k to generate the cyphertext c, after that to get back to the initial message m, Bob will then need to decrypt it utilizing his own key k on cyphertext c.
In a more formal way we can define Symmetric encryption (SKE) as $\prod = (Enc, Dec)$ such that:

- Enc : $\mathscr{M} \times \mathscr{K} \to \mathscr{C}$
- Dec: $\mathscr{C} \times \mathscr{K} \to \mathscr{C}$
- k is uniform over $\mathscr{K}$ (k is chosen according to some distribution)

An encryption scheme must satisfy the correctness requirement:

Definition 1. *$\forall k \in \mathscr{K}, \forall m \in \mathscr{M}$ it holds that $Dec(k, Enc(k, m)) = m$*

Kerchoff's Principle:

Definition 2. *Security should not depend on the secrecy of the algorithm but on the secrecy of the key.*

1.3 Perfect Secrecy

Definition 3. *Let M be any distribution over $\mathscr{M}$ and K be uniform over $\mathscr{K}$ (Then observe C = Enc(K,M) in a distribution over C), we say that (Enc,Dec) = $\prod$ is **perfectly secret** if $\forall M, \forall m \in \mathscr{M}, \forall c \in \mathscr{C} : Pr[M = m] = Pr(M = m|C = c)$ (The probability that M is m is equal to the probability that M is m knowing that C is c, so by knowing the cyphertext, we dont gain additional information).*

Lemma 1. *The following are equivalent:*

- *Perfect Secrecy*
- *M and C are independant*
- $\forall m, m' \in \mathscr{M}, \forall c \in \mathscr{C} : Pr[Enc(k, m) = c] = Pr[Enc(k, m') = c]$ *with k being uniform over $\mathscr{K}$*

1.4 OTP

Let us see if OTP (*One Time Pad*) is perfectly secret
We know that the OTP uses $\oplus$ to generate and later decypher the cyphertext, we have that $K = M = C = \{0, 1\}^N$ with N being the length of the string, we know that:

- Enc (k,m) $= k \oplus m$
- Dec (k,c) $= c \oplus k = (k \oplus m) \oplus k = m$

To prove that it is perfectly secret let us utilize the third lemma:

$$Pr[C = c|M = m'] = Pr[\text{Enc}_k(m') = c] = Pr[m' \oplus K = c] = Pr[K = m' \oplus c] = 2^{-N}$$

and therefore:

$$Pr[Enc(k, m') = c] = 2^{-N}$$

There seem to be some limitations, the key can only be used once and it must as long as the message,lets assume we encrypt m" and m': $c_1 = k \oplus m_1$ $c_2 = k \oplus m_2$ therefore $c_1 \oplus c_2 = m_1 \oplus m_2$, so if I know a pair (m_1, c_1) then I could compute m_2, therefore we cannot encrypt two messages with the same key.

Theorem 1. *Let $\prod$ be a SKE then we have $|\mathscr{K}| \geq |\mathscr{M}|$.*

Proof. Take $\prod$ to be uniform over $\mathscr{M}$. Take any c s.t. Pr[C=c] > 0.
Consider $\mathscr{M}' = \{Dec(k, c) : k \in \mathscr{K}\}$ and assume $|\mathscr{K}| < |\mathscr{M}|$ by contraddiction, then:

$$|\mathscr{M}|' \leq |\mathscr{K}| < |\mathscr{M}| \rightarrow |\mathscr{M}'| < |\mathscr{M}| \rightarrow \exists m \in \mathscr{M} \setminus \mathscr{M}'$$

Now:

$$\text{Pr[M=m]} = |\mathscr{M}|^{-1} \text{ but Pr[M=m — C=c]} = 0$$

$\square$