- Integridade de Mensagens e Autenticação.

Integridade

- Integridade de mensagens é um mecanismo ou serviço usado para verificar a integridade de uma mensagem.
- A Integridade garante que os dados recebidos sejam exatamente iguais aos enviados.

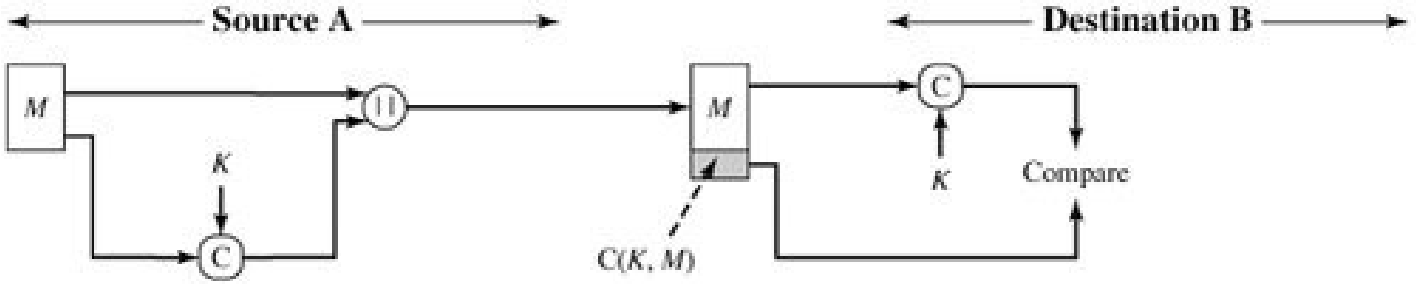
- As duas técnicas criptográficas mais usadas de autenticação de mensagens são:
    - MAC – Message Authentication Code.
    - SHA – Secure Hash Algorithm.

MAC – Message Authentication Code

- É o uso de uma chave secreta *K* para gerar um pequeno bloco de dados de tamanho fixo, conhecido como MAC, que é anexado à mensagem *M*.

- Se A e B compartilham uma chave secreta *K*, então:

$$MAC = C(K, M)$$



(a) Message authentication

Função de Hash

- Diferente de um MAC, um código de hash não usa uma chave *K*, sendo uma função apenas da mensagem de entrada, H(*M*).