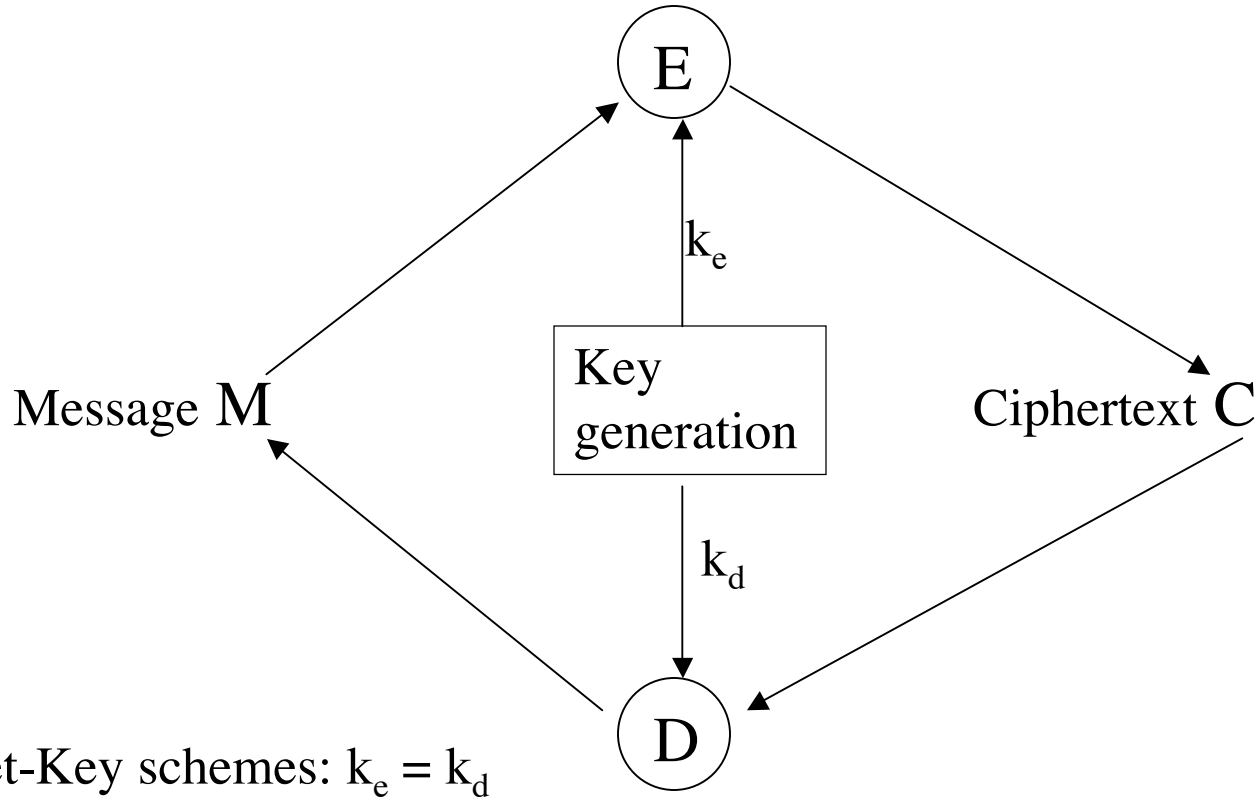
Some diagrams illustrating concepts from IT security

Cryptosystems

Any system: $D_{kd}(E_{ke}(M)) = M$



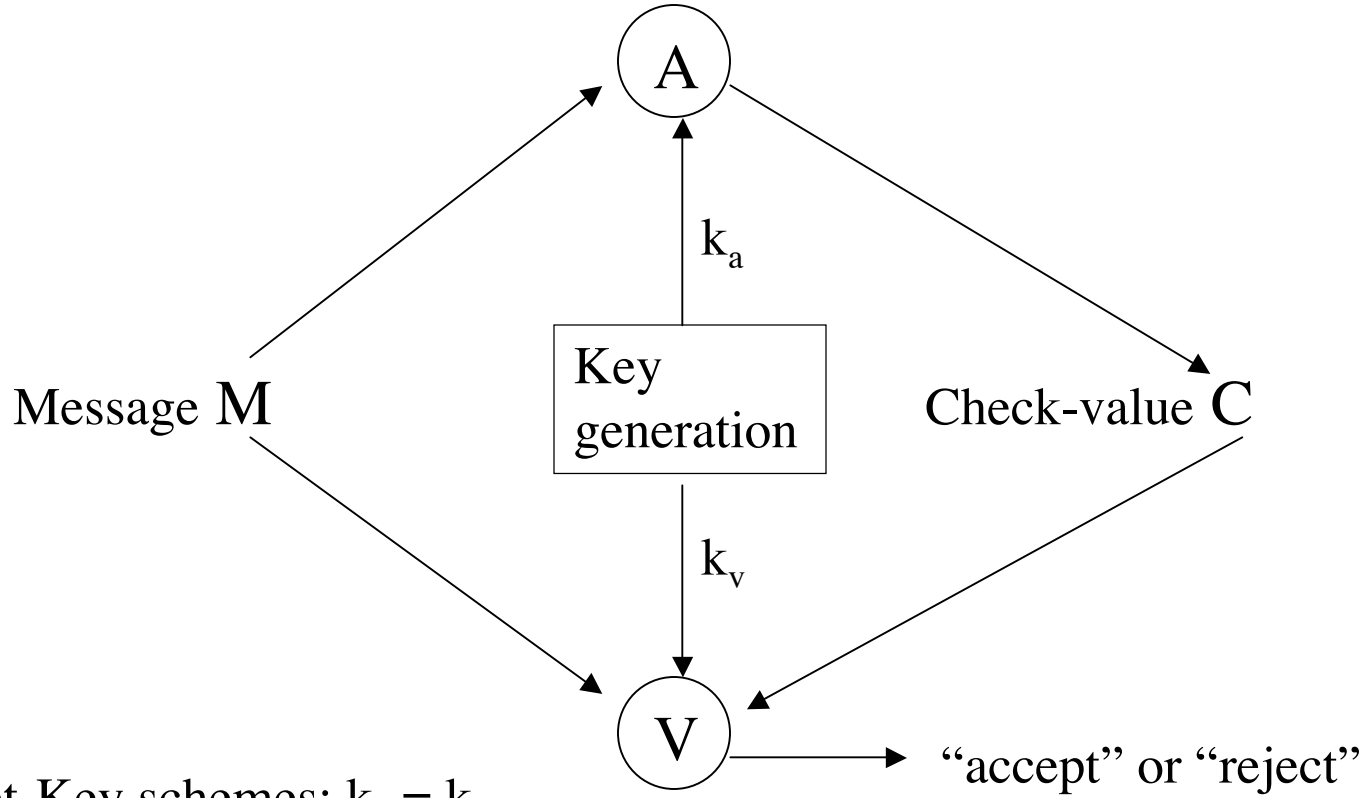
Secret-Key schemes: $k_e = k_d$

Public-key schemes: k_e, k_d different, k_e can be public while k_d is still private

Security: given C (and maybe public key), infeasible to find info on M

Authentication Systems

Any system: $V_{kv}(M, k_v, A_{ka}(M)) = \text{accept}$

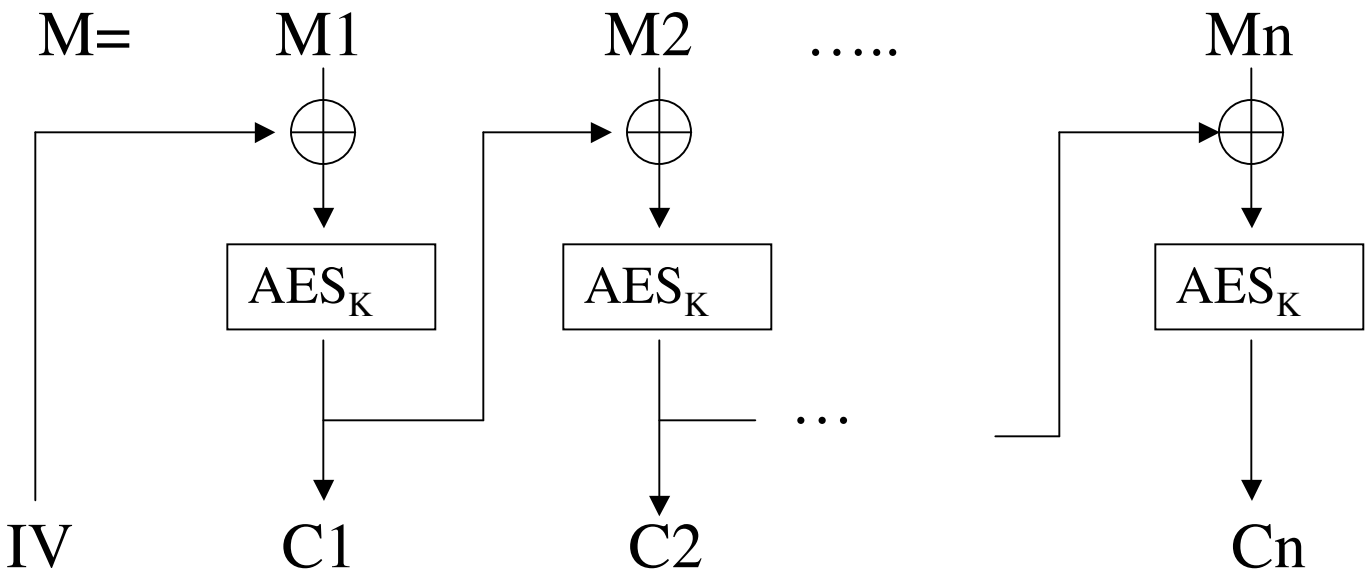


Secret-Key schemes: $k_a = k_v$

Public-key schemes: k_a, k_v different, k_v can be public while k_a is still private

Security: given some authenticated messages, infeasible to find good check value for a NEW message, not sent by legal sender.

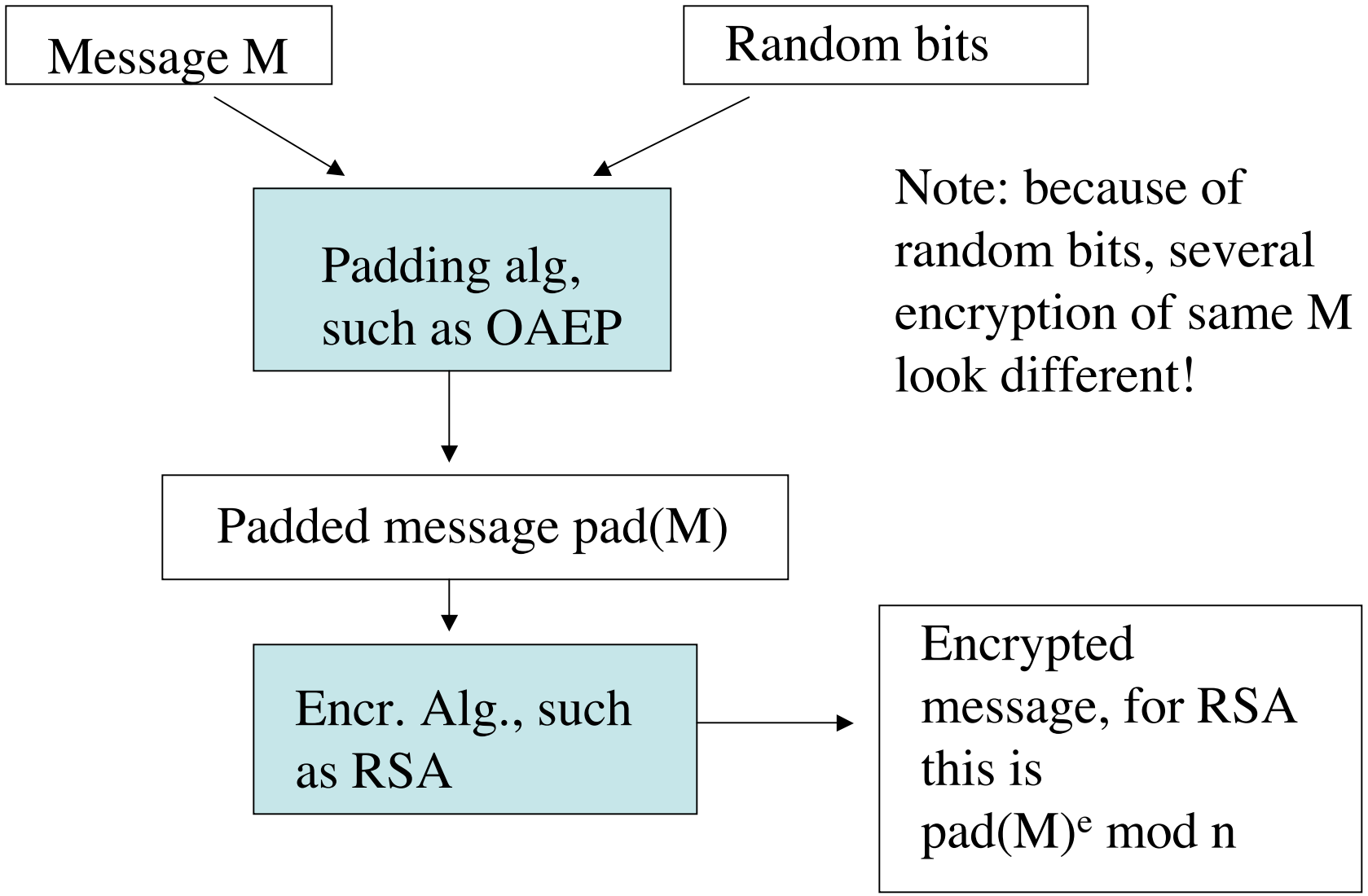
CBC - encryption



IV: Initialization vector. Not secret, is sent as part of ciphertext. Must be a nonce, i.e., must not repeat, use random choice, or sequence number, for instance.

Note: AES can be replaced by any other secure block cipher

Secure usage of public-key encryption, such as RSA



Note: because of random bits, several encryption of same M look different!