

[Appendice \(Tag, appendix\)](#)

[Attaquant](#)

[Attaque](#)

[Authentification \(Authentication\)](#)

[Autorité de certification \(certifying authority\)](#)

[Canal de communication \(Communication channel\)](#)

[Certificat \(Certificate\)](#)

[Certification](#)

[Chiffrement \(Cipher, ciphering\)](#)

[Clé \(Key\)](#)

[Code d'authentification de message \(Message authentication code\)](#)

[Collision \(Collision\)](#)

[Confidentialité \(Privacy\)](#)

[Confusion \(Confusion\)](#)

[Contrefaçon \(forgery\)](#)

[Contrôle d'accès \(Access control\)](#)

[Cryptanalyse \(Cryptanalysis\)](#)

[Cryptogramme \(Ciphertext\)](#)

[Cryptographie \(Cryptography\)](#)

[Cryptologie \(Cryptology\)](#)

[Cryptosystème \(Cryptosystem\)](#)

[Déchiffrement](#)

[Décryptage](#)

[Déduction globale](#)

[Destinataire](#)

[Diffusion](#)

[Échange de clé \(Key exchange\)](#)

[Encodage \(Encoding\)](#)

[Encryptage \(Ciphering\)](#)

[Ennemi](#)

[Enveloppe](#)

[Expéditeur \(Sender\)](#)

[Exposition](#)

[Faible \(Weak\)](#)

[Faux \(Forgery\)](#)

[Fonction à sens unique \(One-way function\)](#)

[Fonction à sens unique avec trappe \(One-way trapdoor function\)](#)

[Fonction de hachage \(Hash function\)](#)

[Générateur de masque \(Key Derivation Function\)](#)

[Générateur pseudo-aléatoire \(Pseudo-random generator\)](#)

[Germe \(Seed\)](#)

[Hard-core bit \(Hard-core bit\)](#)

[Homme au milieu \(Man in the middle\)](#)

[Horodatage \(time-stamp\)](#)

[Imitation \(Forgery\)](#)

[Imitation existentielle \(existential forgery\)](#)

[Imitation sélective \(selective forgery\)](#)

[Imitation universelle \(universal forgery\)](#)

[Identification \(Identification\)](#)

[Infrastructure de gestion de clé \(Public Key Infrastructure\)](#)

[Indistinguabilité \(Indistinguishability\)](#)

[Intégrité \(Integrity\)](#)

[Mascarade](#)

[Modèle de l'oracle aléatoire \(Random oracle model\)](#)

[Modèle standard \(Standard model\)](#)

[Non-répudiation \(Non-repudiation\)](#)

[Opérateur de certification](#)

[Paradoxe des anniversaires](#)

[Preuve à divulgation nulle \(Zero-knowledge proof\)](#)

[Preuve de sécurité \(Security proof\)](#)

[Protocole \(protocol\)](#)

[Rejeu \(Replay\)](#)

[Rencontre au milieu \(Meet in the Middle\)](#)

[Sécurité calculatoire \(Computational security\)](#)

[Sécurité parfaite \(Perfect security\)](#)

[Sécurité rétroactive](#)

[Signature \(Signature\)](#)

[Sphère de confiance](#)

[Substitution](#)

[Suite pseudo-aléatoire \(pseudo-random sequence\)](#)

[Texte clair \(Plaintext\)](#)

[Texte chiffré \(Ciphertext\)](#)

[Tiers de confiance](#)

[\[Retour \]](#)