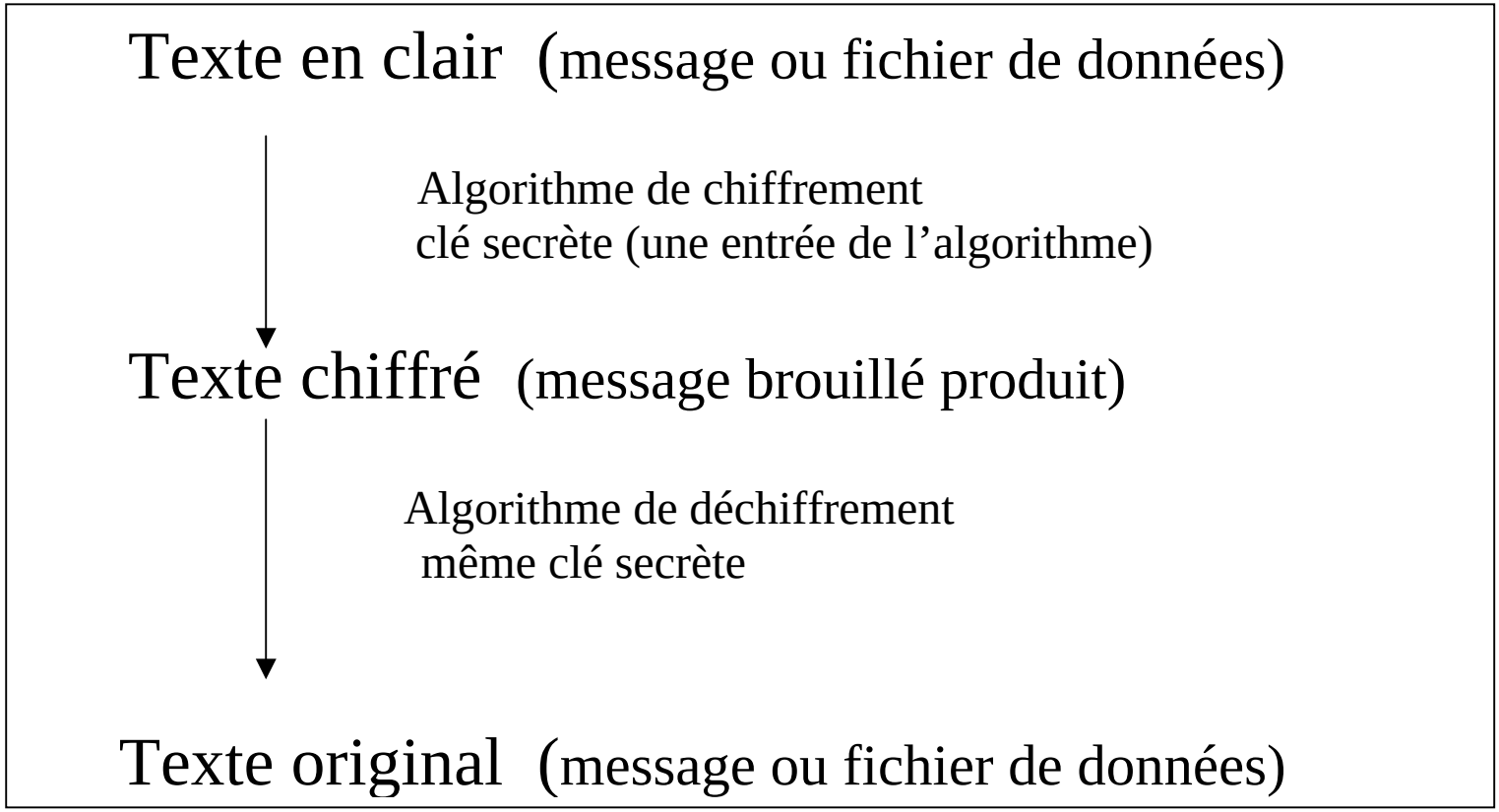
CHIFFREMENT CONVENTIONNEL (ou symétrique)

Principes



Remarque : la sécurité dépend du secret de la clé et non de l'algorithme

Cryptographes

Concepteurs d'algorithmes de chiffrement /déchiffrement avec pour finalité le secret et/ou l'authentification des messages.

Cryptanalystes

trouvent des moyens de casser un code secret afin de trouver l'information

(dépend du schéma de chiffrement et des infos aux mains du casseur)

Déchiffrer un message :

trouver le texte en clair sans connaître la clé secrète ou l'algorithme de chiffrement

Casser un code :

trouver un moyen systématique de déchiffrer un texte chiffré en son original

PRINCIPE FONDAMENTAL

On considère aujourd'hui qu'un algorithme de chiffrement est difficile à casser si aucun des meilleurs cryptanalystes n'arrive à le faire en un nombre polynomial d'opérations par rapport à la taille de la clé.
Ceci implique que de tels algorithmes doivent être publiés.
Garder un algorithme de chiffrement secret rend le déchiffrement plus dur, mais ceci est en général impossible car le code de l'algorithme doit exister dans tout lieu où il est utilisé.

Exceptions : quand un organisme implémente un algorithme propriétaire dans un circuit intégré.
Ex : cartes à puce.

Un peu d'histoire

Les codes secrets ont toujours fasciné le grand public.
Décrypter les dépêches ennemies a très souvent joué un rôle dans l'Histoire, dans la diplomatie, pendant les conflits.
5ème siècle avant J-C : guerre Grèce-Perse : utilisation d'un bâton sur lequel on enroule un parchemin sur lequel on écrit le message
(au préalable, échanger un secret)

Chiffre de César 'substitution monoalphabétique'
Entrée: ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890_
Sortie : DEFGHIJKLMNOPQRSTUVWXYZ1234567890_ABC

ART DE DISSIMULER LES INFORMATIONS
DUWCGHCGLVVLPXOHUCOHVCLQIRUPDWLROV

9ème siècle : la civilisation arabe invente la cryptanalyse. Al Kindi expose le moyen de casser tout chiffrement reposant sur une substitution de lettres. Dans une langue, fréquence importante de certaines lettres
fin du 16ème siècle (1586), mise au point d'un chiffrement appelé substitution polyalphabétique.
Le secret à échanger devient non plus la technique utilisée mais la clé secrète.

DIFFICULTE CALCULATOIRE

Les codes les plus communs ont des algorithmes qui sont bien connus et la clé pour un texte chiffré particulier peut être trouvée à l'aide d'une recherche exhaustive
(mais, pour T-DES, RSA, pas en un temps raisonnable avec les ressources disponibles)

César : 26 clés possibles

Clé de 4 pour chiffrer 40 positions :

40*40*40*40 = 2 560 000 combinaisons possibles

1 combinaison toutes les 13 s : 1 an pour tout

DES - clé de 56 bits : 2^56 = 4 E18 combinaisons

Taille de clé(bits)	Nb clés possibles	Tps requis(1déch/µs)	Tps requis(10^6d /µs)
32	2^32=4,3 .10^9	35,6 mn	2,15 ms
56	2^56=7,2 .10^16	1142 années	10 h
128	2^128=3,4 .10^38	5,4 . 10^24 années	5,4. 10^18 années
168	2^168=3,7 .10^50	5,9 . 10^36 années	5,9. 10^30 années

TYPES d'ATTAQUES

Seul le texte chiffré est disponible
- essayer différentes clés, voir si résultat reconnu
- mieux si plus de cryptogrammes disponibles : essais statistiques

Texte chiffré et texte en clair correspondant disponibles
- on peut savoir que certains motifs de texte apparaîtront dans un message

Texte en clair choisi
- l'analyste arrive à insérer un message choisi dans un système source, sélectionne des motifs prévus pour révéler la structure de la clé

Choisir clé, texte en clair et observer variations dans le chiffrement

TYPES DE FONCTIONS CRYPTOGRAPHIQUES

Clé secrète (Conventionnel ou Symétrique)

- clés identiques pour le chiffrement et le déchiffrement des données.
- Texte chiffré et texte en clair de même longueur
- Utilisée pour la transmission et le stockage confidentialité
- peut être utilisée pour l'authentification
- génère code d'authentification de message

Clé publique (publique-privée, asymétrique)

- inventée en 1975
- la clé publique peut être utilisée par tous pour l'envoi d'un message
- la clé privée peut être utilisée pour une 'signature électronique

Fonction de hachage (condensé de message ou fonction à sens unique

- (hachage de mots de passe)

MODES DE CHIFFREMENT PAR BLOCS

Traitent un bloc de taille fixe de bits de données à la fois.

DES et IDEA traitent des codes de 64 bits comme valeurs d'entrée

- il y a 2^64 = 7 000 000 000 000 valeurs
- chacune est transformée en un unique texte chiffré.
  - ➢ l'unicité est assurée par une série d'étapes réversibles
- la transformation apparaît comme aléatoire
  - ➢ changer un bit en entrée change presque la moitié des bits en sortie

OPERATIONS SUR LES BLOCS

Substitutions

- substituer chaque bloc b de n bits par un autre de même taille
- Table : b ➔B(b) demande 2^n vecteurs de n bits
  - >n = 8 bits (facile), n = 64 bits (trop large)
- algorithme réversible d'opérations inversibles :
  - > B(b) = b (+) c, (+) est l'opération XOR, c est constant
  - >B(b) = b (+) c mod2^n
  - >B(b) = bxc mod2^n quand c est impair

Théorie des nombres : si 2^n et c n'ont pas de facteur commun, il existe u tel que b = B(b) x u mod2^n.

Permutations

- Facile à implémenter en hardware, difficile en soft

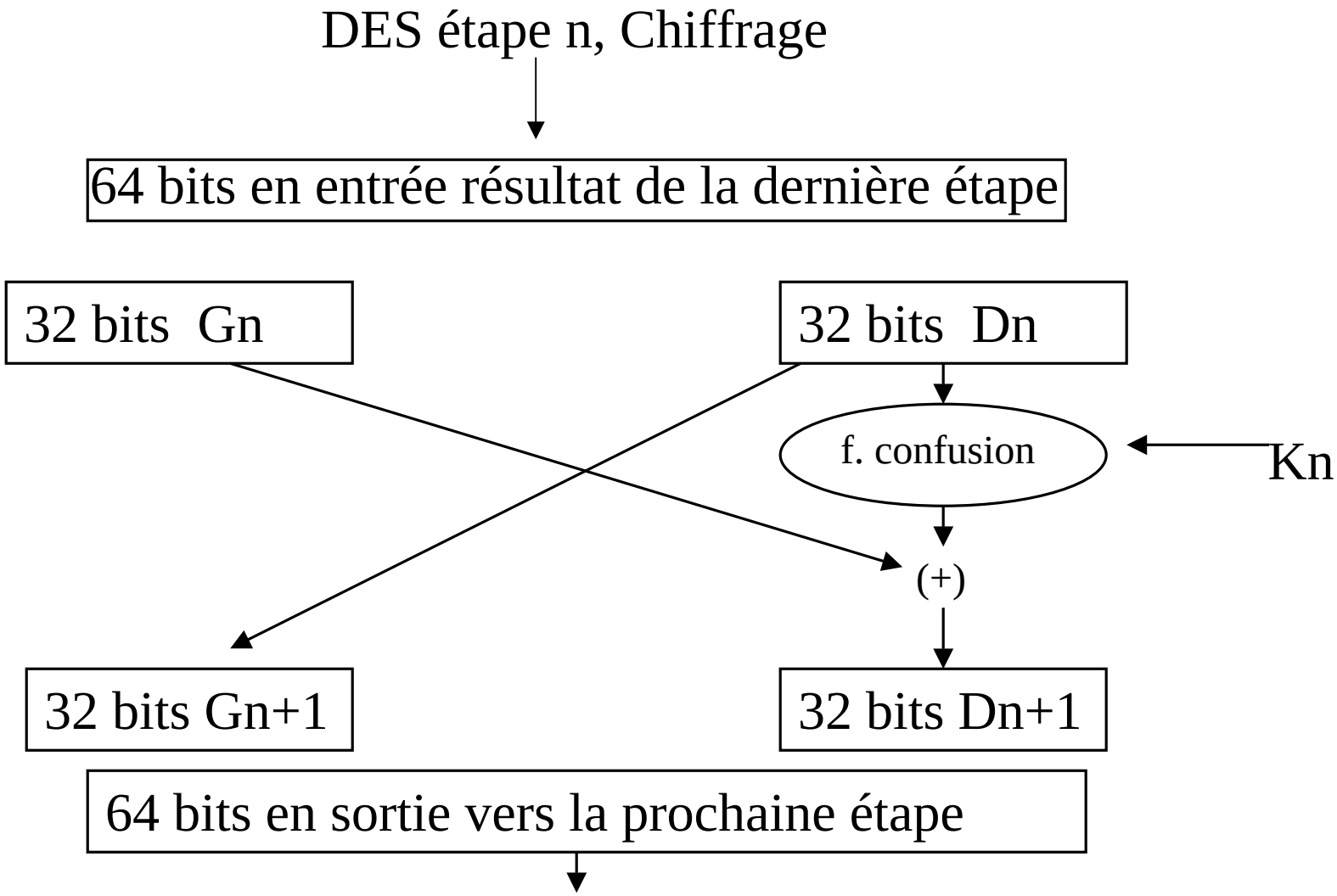
DES (Data Encryption Standard ou Standard de Chiffrement de Données)

Clé à 56 bits
Taille fixe des blocs de données = 64 bits

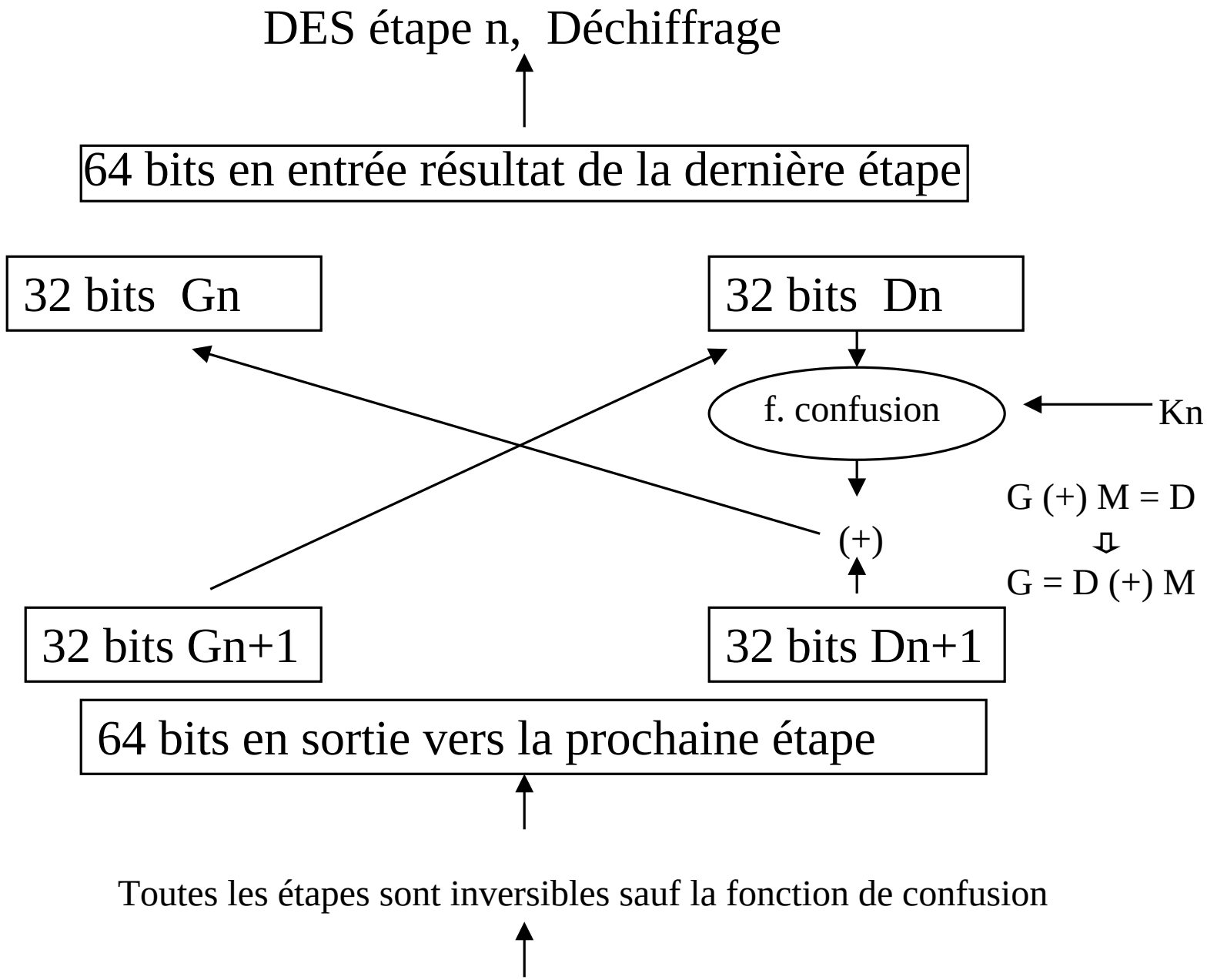
64 bits pour la permutation initiale
16 itérations du système Feistel

chaque étape utilise une fonction de confusion .

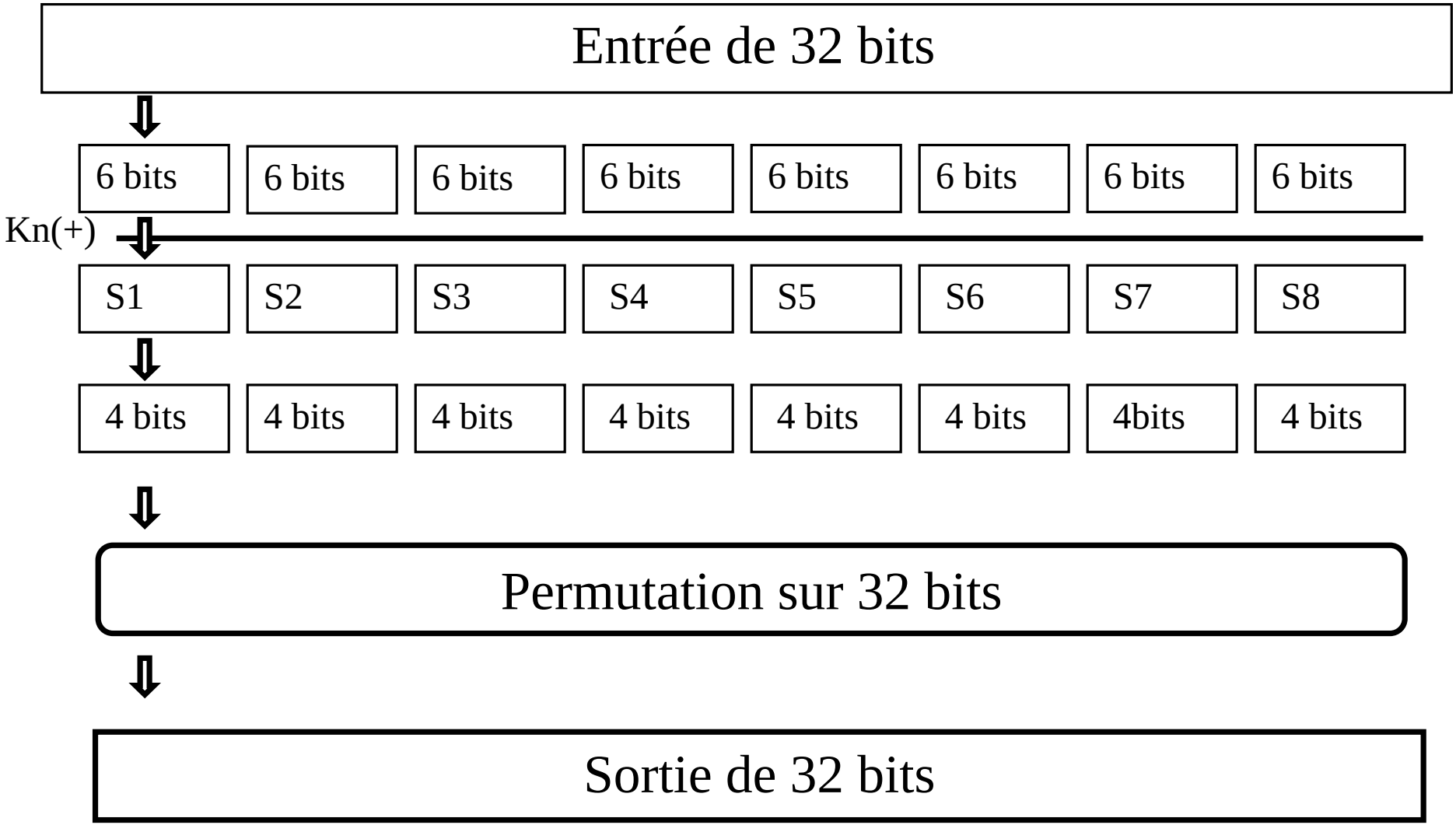
à la fin
Permutation finale : inverse de l’initiale
Ces permutations des données ainsi que la clé de 56 bits sont utilisées dans un but de rendre leur découverte impossible .



Pourquoi ceci est-il réversible pour toute fonction de confusion ?


DES étape n, Déchiffrage
64 bits en entrée résultat de la dernière étape
32 bits Gn
32 bits Dn
f. confusion
Kn
G (+) M = D
⇩
G = D (+) M
(+)
32 bits Gn+1
32 bits Dn+1
64 bits en sortie vers la prochaine étape
Toutes les étapes sont inversibles sauf la fonction de confusion

DES – Fonction de confusion



DES – Boites de transformations S

Les boites S sont au nombre de 8 à chacune des 16 étapes.
A chaque entrée de 6 bits, S fait correspondre 4 bits en sortie.
Les 128 tables de correspondance sont toutes différentes.

Chaque ensemble de 4 bits en sortie peut être le résultat par la transformation S de différentes suites de valeurs de 4 bits en entrée.

La transformation S n'est donc pas une fonction réversible.
Mais cette propriété n'est pas obligatoire pour S pour assurer le déchiffrement.

Le processus de choix des boîtes S reste un secret de l'algorithme.

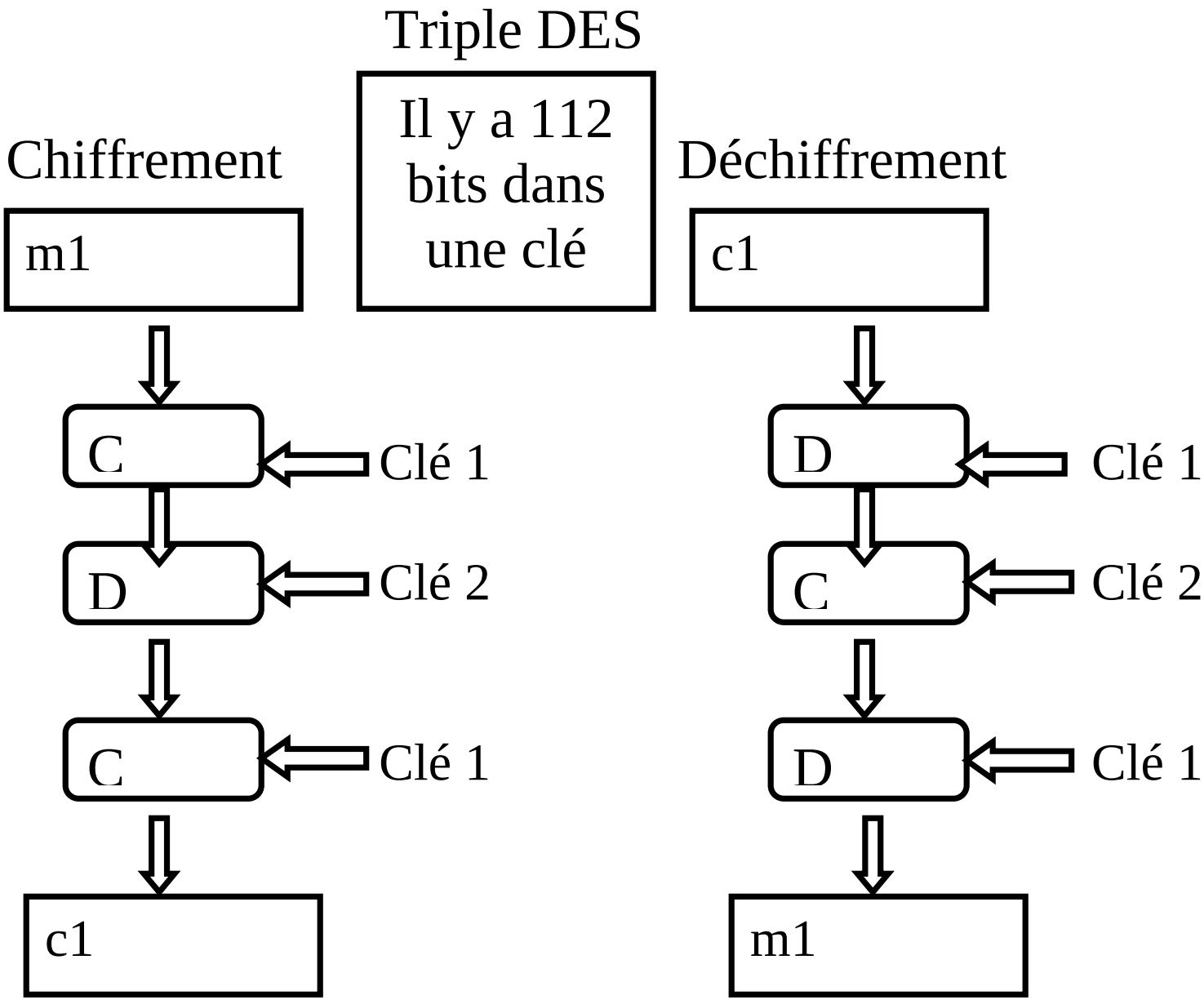
Question : Peut-on casser DES ?

CASSER L'ALGORITHME DES ?

1998 : le système de chiffrement DES est décrypté – pour moins de 250 000 $ - par une simple association de particuliers.
Le processeur spécialisé exécute 1000 déchiffrements par nanoseconde,
sur des clés de 56 bits trouve la bonne clé au bout de 3 jours.

Réponse : utiliser des clés plus longues. Des clés de 128 bits …

Déjà, T-DES (Triple-DES) utilise effectivement une clé de 112 bits


Triple DES
Il y a 112 bits dans une clé
Chiffrement
m1
C
Clé 1
D
Clé 2
C
Clé 1
c1
Déchiffrement
c1
D
Clé 1
C
Clé 2
D
Clé 1
m1

IDEA(International Data Encryption Algorithm)/ DES

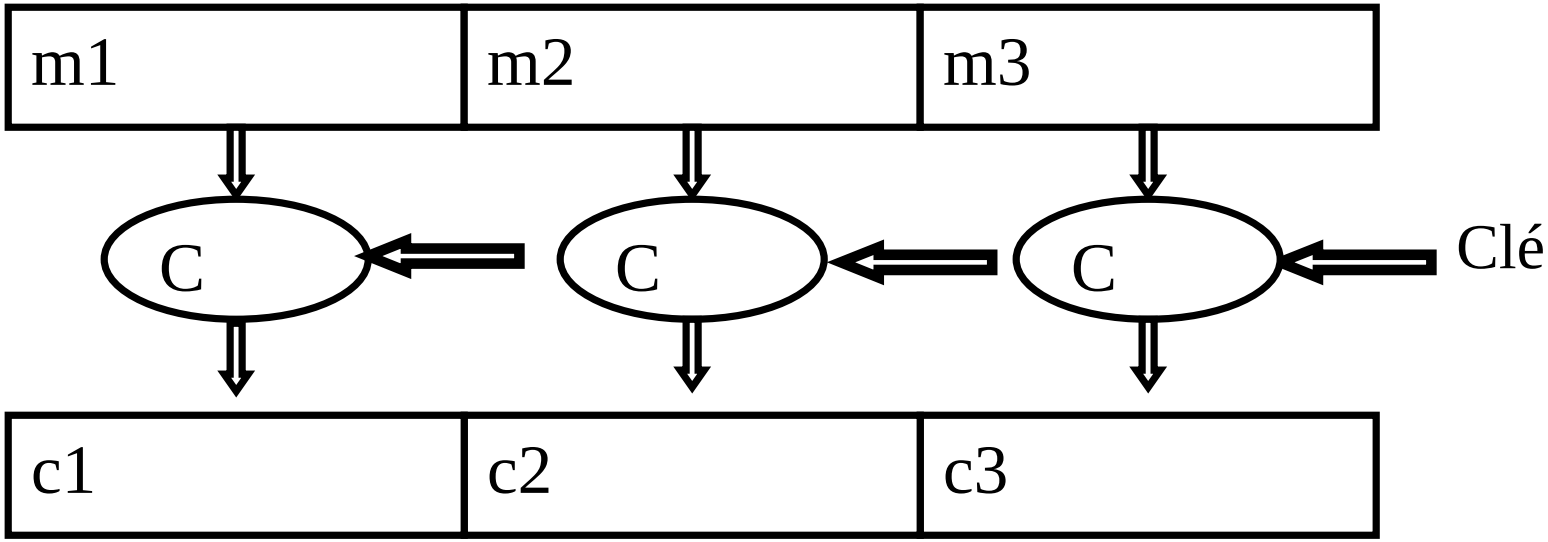
Clé de 128 bits / clé de 56 bits. 3.4 E38 / 7 E16 valeurs possibles
4 194 304 fois plus de temps que DES
Si une recherche exhaustive de clé pour DES prend une heure, pour IDEA, elle prendrait 500 années.

Opérations primitives appliquent 16 bits sur 16 bits au lieu de 6 sur 4.
Utilisent des opérations mathématiques plutôt que des transformations S

Développement de nouveaux algorithmes : Blowfish, RC5, CAST-128

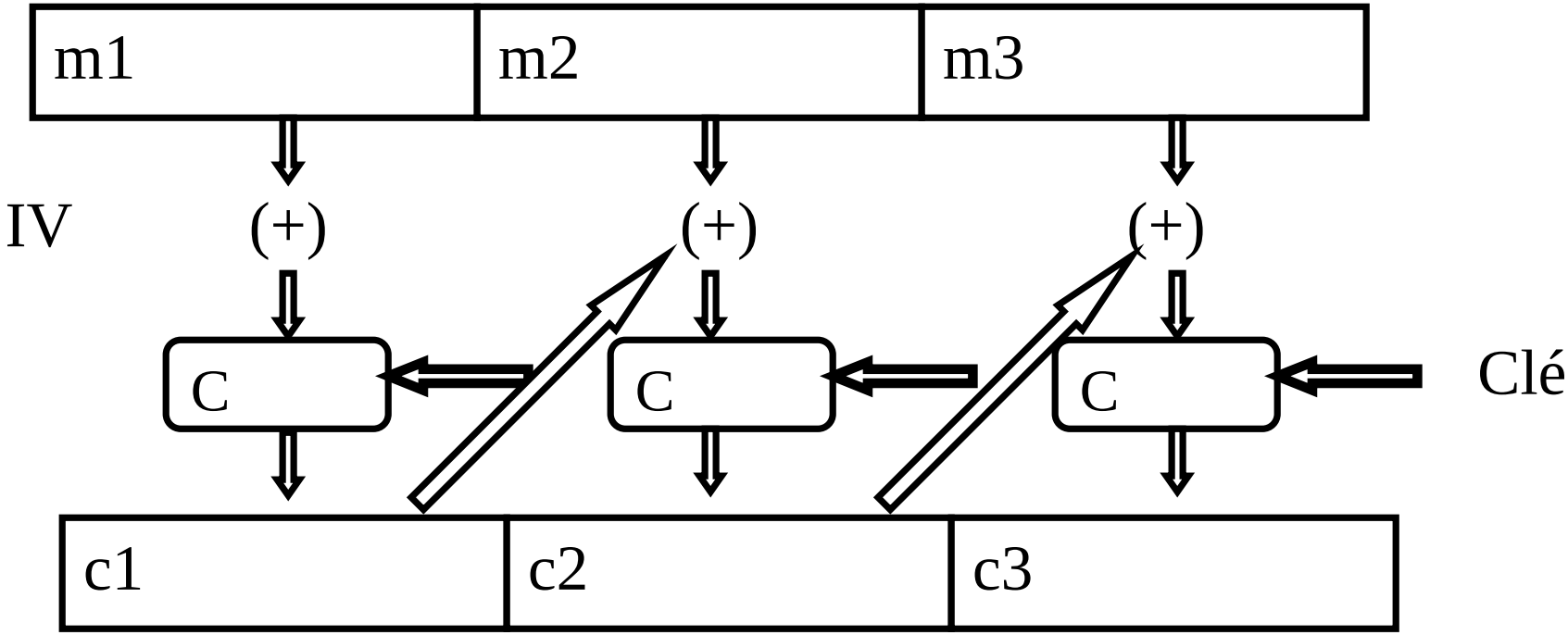
NIST(National Institute of Standards and Technologies) a choisi, en octobre 2000 l'AES (Advanced Encryption Standard ou standard de chiffrement avancé)
AES utilise des clès de 128, 192 et 256 bits et des blocs de 128 bits.

ECB (Electronic CodeBook ou livre de code électronique)



Chaque segment de 64 bits est remplacé, à l'aide d'une opération de chiffrement 'C'utilisant la même clé, par un autre segment en sortie. Des messages identiques produisent des textes chiffrés identiques.

CBC (Cipher Block Chaining ou chiffrement par blocs chainés)



Le 1er segment de 64 bits du message est XORé avec le vecteur initial (IV). Pour ceux qui suivent, chacun est XORé avec le segment chiffré précédent.

ECB (livre de code électronique)

Les blocs chiffrés répétés révèlent les informations structurées.
Les blocs peuvent être réarrangés, dupliqués, supprimés par un attaquant sans que l’on s’en aperçoive.

CBC (Chiffrement par blocs chaîné)

Changer des bits dans c12 produit des changements des mêmes bits dans m13.
On s’en protège en incluant un CRC ou un MIC dans le message.