NORME INTERNATIONALE

ISO 10126-1

Première édition
1991-11-01

Banque — Procédures de chiffrement de messages (service aux entreprises) —

Partie 1: Principes généraux

Banking — Procedures for message encipherment (wholesale) —

Part 1: General principles

Numéro de référence
ISO 10126-1:1991(F)

Sommaire

Organisation internationale de normalisation
Case Postale 56 • CH-1211 Genève 20 • Suisse
Imprimé en Suisse

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

La Norme internationale ISO 10126-1 a été élaborée par le comité technique ISO/TC 68, *Banque et services financiers liés aux opérations bancaires*, sous-comité SC 2, *Opérations et procédures*.

L'ISO 10126 comprend les parties suivantes, présentées sous le titre général *Banque — Procédures de chiffrement de messages (service aux entreprises)*:

— *Partie 1: Principes généraux*

— *Partie 2: Algorithme DEA*

L'ISO 10126 est le fruit des travaux de l'ANSI et est un développement de l'ANSI X9.23 (1988), *Financial Institution: Encryption of Wholesale Financial Messages*, avec laquelle elle reste compatible.

Les quatre annexes de la présente partie de l'ISO 10126 sont destinées à faciliter sa mise en œuvre.

a) L'annexe A donne la procédure à suivre pour l'examen d'autres algorithmes de chiffrement.

b) L'annexe B donne des exemples des différentes techniques de filtrage décrites dans la présente partie de l'ISO 10126.

c) L'annexe C permet de comparer les effets des filtres décrits dans la présente partie de l'ISO 10126 et, grâce au facteur d'expansion, indique la relation entre le nombre de bits transmis et ceux reçus.

d) L'annexe D donne des exemples des trois méthodes de chiffrement et de déchiffrement des éléments de chiffrement d'un message qui sont décrites dans la présente partie de l'ISO 10126.

L'annexe A fait partie intégrante de la présente partie de l'ISO 10126. Les annexes B, C et D sont données uniquement à titre d'information.

Introduction

La présente partie de l'ISO 10126 prescrit une méthode de chiffrement et de déchiffrement des messages financiers dans leur intégralité ou partiellement, par l'utilisation du chiffrement au niveau applicatif, dans le but d'en assurer la confidentialité.

Le niveau de sécurité fourni par la présente partie de l'ISO 10126 dépend a) de la sécurité liée à l'algorithme utilisé pour le chiffrement et à la mise en place de cet algorithme dans le cadre des procédures fixées par la présente partie de l'ISO 10126 et b) du fonctionnement d'un système sécurisé de gestion des clés.

Les algorithmes particuliers pouvant être utilisés avec la présente partie de l'ISO 10126 sont décrits dans l'ISO 10126-2. Une Norme internationale appropriée relative à la gestion des clés est décrite dans l'ISO 8732.

Banque — Procédures de chiffrement de messages (service aux entreprises) —

Partie 1:
Principes généraux

1 Domaine d'application

Les procédures décrites ici sont conçues pour protéger, par le chiffrement, des messages financiers (messages entiers ou éléments à chiffrer) échangés dans n'importe quelle architecture de communication. De telles architectures s'étendent aux capacités de transmission différée, au telex, à un nombre quelconque de nœuds et à des réseaux privés ou publics.

Dans la mesure où un texte chiffré peut avoir une influence néfaste sur les processus de communication des réseaux financiers existants, la présente partie de l'ISO 10126 fournit un moyen permettant de transmettre le message chiffré à travers un certain nombre de réseaux sans qu'il puisse être incorrectement interprété comme étant une information de protocole de communication [par exemple, STX (début de texte), EOT (fin de transmission)].

La confidentialité des données de message financier, sous une forme structurée ou non, est protégée grâce à l'utilisation appropriée de la présente partie de l'ISO 10126.

Les techniques décrites n'assurent pas la protection de l'intégrité (c'est-à-dire la protection contre toute modification, substitution ou rejeu). La protection de l'intégrité des données est l'objet de l'ISO 8730 et de l'ISO 8731. Le domaine d'application de la présente partie de l'ISO 10126 ne porte pas non plus sur les formats de message.

2 Références normatives

Les normes suivantes contiennent des dispositions qui, par suite de la référence qui en est faite, constituent des dispositions valables pour la présente partie de l'ISO 10126. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes des accords fondés sur la présente partie de l'ISO 10126 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur à un moment donné.

ISO 646:1983, *Traitement de l'information — Jeu ISO de caractères codés à 7 éléments pour l'échange d'information.*

ISO 8730:1990, *Opérations bancaires — Spécifications liées à l'authentification des messages.*

ISO 8731-1:1987, *Banque — Algorithmes approuvés pour l'authentification de messages — Partie 1: DEA.*

ISO 8731-2:1987, *Banque — Algorithmes approuvés pour l'authentification des messages — Partie 2: Algorithme d'authentification des messages.*

ISO 8732:1988, *Banque — Gestion de clés.*

ISO 10126-2:1991, *Banque — Procédures de chiffrement de messages (service aux entreprises) — Partie 2: Algorithme DEA.*

3 Définitions

Pour les besoins de la présente partie de l'ISO 10126, les définitions suivantes s'appliquent.

3.1 baudot: Code d'information de caractères à cinq bits (non compris les bits de début et de fin facultatifs); Alphabet CCITT Numéro 2.

3.2 bloc: Unité de données d'une longueur spécifiée.

3.3 cryptogramme: Informations chiffrées.

3.4 couple d'interlocuteurs: Deux entités logiques d'accord pour échanger des données.

3.5 clé de chiffrement; clé: Paramètre complémentaire d'un algorithme servant au chiffrement ou au déchiffrement.

3.6 unité de données: Vecteur binaire de K bits notés (B1, B2, ..., BK).

3.7 déchiffrement: Transformation inverse du chiffrement réversible correspondant.

3.8 élément chiffré: Élément de chiffrement chiffré.

3.9 chiffrement: Transformation chiffrée de données aboutissant à un cryptogramme.

3.10 élément à chiffrer: Groupe de caractères contigus d'un texte clair qui doivent être chiffrés.

3.11 filtrage: Processus de codage d'un texte binaire en un format insensible aux caractères de commande.

3.12 message financier: Communication comportant des informations à caractère financier.

3.13 vecteur d'initialisation (IV): Nombre servant de point de départ au chiffrement d'une séquence de données. Il accroît la sécurité en introduisant une variation cryptographique supplémentaire et facilite également la synchronisation de l'équipement de chiffrement.

3.14 séquence de texte initiale (ITS): Vecteur binaire de n bits pouvant être placé devant un message.

3.15 clé: Voir clé de chiffrement.

3.16 entité logique: Une ou plusieurs entités physiques formant l'un des membres d'un couple d'interlocuteurs.

3.17 message: Communication comportant une ou plusieurs transactions ou des informations apparentées.

3.18 bit(s) le(s) plus significatif(s): Bit(s) le(s) plus à gauche d'un vecteur binaire.

3.19 octet: Groupe de huit chiffres binaires numérotés de gauche à droite: B1, B2, ..., B8.

3.20 remplissage: Un ou plusieurs bits ajoutés à la fin d'un message afin que le message contienne un multiple exact du nombre de bits requis par le processus de filtrage ou l'algorithme de chiffrement.

3.21 texte clair: Informations non chiffrées.

3.22 destinataire: Entité logique autorisée à déchiffrer un message reçu.

3.23 expéditeur: Entité logique responsable de l'envoi d'un message chiffré.

4 Application

4.1 Protection fournie

La confidentialité des données d'un message financier est protégée grâce à l'utilisation correcte de la présente partie de l'ISO 10126. La présente partie de l'ISO 10126 fournit une méthode de protection pour les données de messages structurés et non structurés. La protection de la confidentialité est assurée entre deux entités logiques. Les entités logiques d'une communication sont l'expéditeur et le destinataire.

4.2 Fonctionnement général

4.2.1 Traitement

L'expéditeur d'un message financier doit créer un cryptogramme en appliquant le processus de chiffrement décrit à l'article 5 soit au message clair entier soit à des éléments à chiffrer contenus dans le message, en utilisant un système sûr de gestion des clés. Le message est alors envoyé au destinataire. Le destinataire doit déchiffrer le cryptogramme en appliquant les procédures de déchiffrement décrites à l'article 5.

Noter que le processus cryptographique est sensible à la séquence dans laquelle le texte clair est chiffré et que la séquence doit être identique au moment du chiffrement et du déchiffrement.

S'il est nécessaire de procéder ultérieurement au déchiffrement d'un message entier ou d'éléments à chiffrer, un journal de contrôle doit contenir suffisamment d'informations pour récupérer la clé, le message et toute autre information utilisée dans les processus cryptographiques.

Lorsqu'un message financier est à la fois authentifié et chiffré, le message doit être authentifié avant le chiffrement et des clés différentes doivent être utilisées pour le chiffrement et l'authentification.

4.2.2 Méthodes de communication

La présente partie de l'ISO 10126 peut servir à chiffrer des messages financiers entiers ou des éléments à chiffrer contenus dans des messages

transmis par n'importe quel moyen de communication à travers un nombre quelconque de nœuds de réseaux privés ou plublics.

5 Chiffrement et déchiffrement de messages entiers et d'éléments à chiffrer

5.1 Généralités

Les messages entiers et les éléments à chiffrer doivent être chiffrés et déchiffrés conformément à l'ISO 10126-2. Il existe quatre méthodes de chiffrement permises par la présente partie de l'ISO 10126, à savoir le chiffrement du message entier et trois méthodes de chiffrement d'éléments à chiffrer. Plusieurs messages utilisant différentes clés, différents modes de fonctionnement, ou différentes méthodes de chiffrement (voir 5.3) et différents filtres (voir l'article 6) peuvent être combinés dans une seule transmission.

5.2 Chiffrement et déchiffrement de messages entiers

Lorsqu'un message entier doit être chiffré, tout le texte clair autre que les informations d'en-tête et de fin (par exemple, les informations ajoutées par un réseau à des fins de transmission) doit être chiffré. La séquence de texte initial (si elle existe), le message entier incluant le MAC (s'il existe) et la zone de remplissage (si elle existe) doivent être chiffrés comme formant un tout. Après le chiffrement, le cryptogramme peut être filtré conformément à l'article 6. Lorsqu'un message entier doit être déchiffré, tout le cryptogramme est déchiffré comme formant un tout.

5.3 Chiffrement et déchiffrement des éléments à chiffrer

Trois méthodes de chiffrement et de déchiffrement des éléments à chiffrer contenus dans un message sont permises par la présente partie de l'ISO 10126.

Méthode 1: Les éléments à chiffrer sont chiffrés indépendamment en éléments chiffrés. Les éléments chiffrés sont déchiffrés indépendamment en éléments à chiffrer (voir 5.3.2).

Méthode 2: Les éléments à chiffrer sont concaténés et chiffrés comme une chaîne unique de données. La chaîne de cryptogramme qui en résulte est transmise dans le message comme une chaîne unique. La chaîne de cryptogramme est déchiffrée et les éléments à chiffrer sont insérés dans le texte du message (voir 5.3.3.1).

Méthode 3: Les éléments à chiffrer sont concaténés et chiffrés comme une chaîne unique de données. La chaîne de cryptogramme qui en résulte est divisée en sous-chaînes de cryptogramme pour transmission à l'intérieur du message. Les sous-chaînes de cryptogramme sont concaténées et déchiffrées comme une chaîne unique. Les éléments à chiffrer qui en résultent sont insérés dans le texte du message (voir 5.3.3.2).

Après le chiffrement, le cryptogramme peut être filtré conformément à l'article 6. Voir l'annexe D comportant des exemples de ces trois méthodes. La même clé, le même algorithme et mode de fontionnement, la même méthode de chiffrement et le même filtre (s'il est mis en œuvre) doivent être utilisés pour chaque élément à chiffrer contenu dans un message particulier.

Le chiffrement des éléments à chiffrer n'offre pas la même protection que le chiffrement de message entier, par exemple le contexte des éléments chiffrés peut donner à une entité non autorisée des indices sur le texte clair sous-jacent.

5.3.1 Séparateurs de zone

Des séparateurs explicites ou implicites sont nécessaires pour délimiter chaque élément à chiffrer, élément chiffré, chaîne de cryptogramme et sous-chaîne de cryptogramme. Des séparateurs pour chaque élément à chiffrer sont nécessaires afin que l'application puisse déterminer les éléments à chiffrer. Des séparateurs pour chaque élément chiffré, chaîne de cryptogramme et sous-chaîne de cryptogramme sont nécessaires afin que l'application puisse déterminer le cryptogramme devant être déchiffré.

Chaque élément à chiffrer peut être délimité soit implicitement soit explicitement dans un message de texte clair. Après le chiffrement, un message peut contenir des éléments chiffrés, une chaîne de cryptogramme ou des sous-chaînes de cryptogramme. Chaque élément à chiffrer chiffré ou sous-chaîne de cryptogramme peut être délimité soit implicitement soit explicitement dans un message. Une chaîne de cryptogramme contenue dans un message peut être délimitée soit explicitement soit implicitememt.

Les paragraphes 5.3.2 et 5.3.3 décrivent les trois méthodes de traitement des éléments à chiffrer utilisant les séparateurs explicites. Les mises en œuvre utilisant les séparateurs implicites doivent traiter les éléments à chiffrer, les éléments chiffrés, les chaînes de cryptogramme et les sous-chaînes de cryptogramme d'une façon équivalente à celle de l'une des trois méthodes.

5.3.1.1 Séparateurs implicites

Un élément à chiffrer, un élément chiffré, une chaîne de cryptogramme ou une sous-chaîne de cryptogramme est délimité implicitement, pour les besoins de la présente partie de l'ISO 10126, si sa position dans le message est fixée ou identifiée

sans ambiguïté par les règles de format et si l'expéditeur et le destinataire sont convenus au préalable de son utilisation.

5.3.1.2 Séparateurs explicites

En l'absence de séparateurs implicites, des séparateurs explicites doivent être utilisés pour identifier le début et la fin des éléments à chiffrer, des éléments chiffrés, d'une chaîne de cryptogramme ou de sous-chaînes de cryptogramme. Les séparateurs explicites sont réservés. Les séparateurs explicites suivants sont établis pour

a) Éléments à chiffrer: QE- et -EQ

   Par exemple: QE- élément à chiffrer -EQ

b) Éléments chiffrés: QC- et -CQ

   Par exemple: QC- élément chiffré -CQ

c) Chaînes ou sous-chaînes de cryptogramme: QC- et -CQ

   Par exemple: QC- chaîne de cryptogramme -CQ

   ou: QC- sous-chaîne de cryptogramme -CQ

5.3.2 Chiffrement et déchiffrement pris séparément des éléments à chiffrer (méthode 1 de 5.3)

Les séparateurs des éléments à chiffrer, QE- et -EQ, ne doivent pas être inclus dans le processus de chiffrement et doivent être remplacés par les séparateurs des éléments chiffrés QC- et -CQ respectivement. Le filtrage peut s'effectuer sur les éléments chiffrés comme décrit à l'article 6, avant d'ajouter les séparateurs QC- et -CQ.

Chaque élément chiffré doit être placé dans le message là où se trouvait l'élément à chiffrer correspondant. Les éléments chiffrés peuvent être plus longs que leurs éléments à chiffrer correspondants pour les raisons suivantes:

a) il se peut que le mode de chiffrement ait nécessité le remplissage du texte clair avant le chiffrement;

b) il se peut que le filtrage, qui entraîne l'expansion des données, ait été utilisé.

Le destinataire défiltre (si nécessaire) et déchiffre indépendamment tous les éléments chiffrés délimités par les séparateurs QC- et -CQ. Chaque élément à chiffrer du texte clair doit être inséré à la place de l'élément chiffré correspondant. Les séparateurs QC- et -CQ doivent être remplacés par les séparateurs QE- et -EQ respectivement.

5.3.3 Chiffrement et déchiffrement des éléments à chiffrer concaténés

Les éléments à chiffrer peuvent être assemblés séquentiellement et chiffrés comme une chaîne unique de données. Après chiffrement, le cryptogramme peut être filtré conformément à l'article 6.

5.3.3.1 Chaînes de cryptogramme (méthode 2 de 5.3)

Le cryptogramme formé à partir du chiffrement à la fois des éléments à chiffrer concaténés et de leurs séparateurs -EQ peut être placé dans un message en tant que chaîne unique de cryptogramme. La chaîne de cryptogramme doit être délimitée par les séparateurs QC- et -CQ. Les séparateurs QE- demeurent dans la portion en clair du message servant de repères (de position).

Le destinataire déchiffre le cryptogramme délimité par les séparateurs QC- et -CQ comme une chaîne unique afin de produire un assemblage d'éléments à chiffrer concaténés, chacun muni d'un séparateur de fin -EQ. Chaque élément à chiffrer et son séparateur -EQ doivent être placés séquentiellement dans le texte clair à l'endroit suivant son séparateur correspondant QE-. Par exemple, le premier élément à chiffrer et son séparateur -EQ sont placés après le premier séparateur QE- dans le message clair et le deuxième élément à chiffrer et son séparateur -EQ sont placés après le deuxième séparateur QE- dans le message clair. Les séparateurs QC- et -CQ ainsi que le cryptogramme sont rejetés.

5.3.3.2 Sous-chaînes de cryptogramme (méthode 3 de 5.3)

Le cryptogramme formé à partir du chiffrement des éléments à chiffrer concaténés sans séparateurs peut être divisé en sous-chaînes de cryptogramme qui sont insérées à la place des éléments à chiffrer dans le message. Lorsque le cryptogramme est inséré à la place d'un élément à chiffrer, chaque bit de l'élément à chiffrer est remplacé par un seul bit de cryptogramme, choisi séquentiellement, à l'exception du dernier élément à chiffrer qui contient tous les bits de cryptogramme restants. Chaque sous-chaîne de cryptogramme doit être délimitée par les séparateurs QC- et -CQ qui remplacent dans le message les séparateurs QE- et -EQ respectivement.

Le destinataire rassemble toutes les sous-chaînes de cryptogramme sans les séparateurs correspondants, séquentiellement, pour former une chaîne de cryptogramme. La chaîne de cryptogramme est alors déchiffrée et divisée en éléments à chiffrer qui sont insérés à la place des sous-chaînes de cryptogramme dans le message. Par exemple, si la première sous-chaîne de cryptogramme du message est de 16 bits, ces bits sont remplacés par les

16 premiers bits de la chaîne du cryptogramme déchiffré. Si la deuxième sous-chaîne de cryptogramme du message est de 40 bits, ces bits sont remplacés par les 40 bits suivants de la chaîne du cryptogramme déchiffré. Ce processus se poursuit jusqu'à ce que la dernière sous-chaîne de cryptogramme soit atteinte. Tous les bits de la dernière sous-chaîne de cryptogramme sont remplacés par les bits restants de la chaîne du cryptogramme déchiffré. Enfin, les séparateurs QC- et -CQ doivent être remplacés dans le message par les séparateurs QE- et -EQ respectivement.

6 Transmission transparente des données chiffrées

6.1 Introduction

Le résultat du processus de chiffrement est une chaîne binaire pseudo-aléatoire. Alors

a) Les systèmes de communication appliquant le codage de caractères ISO 646 peuvent interpréter ou reconnaître une partie de cette sortie binaire pseudo-aléatoire comme étant des fonctions de commande. Ces fonctions de commande peuvent avoir un effet défavorable sur le fonctionnement du service de transmission (par exemple, des caractères parasites XON/XOFF ou Fin de Fichier).

b) Les systèmes de communication appliquant le codage de caractères Baudot peuvent interpréter ou reconnaître une partie du cryptogramme comme étant des chaînes de caractères utilisées par les services de transmission comme chaînes de contrôle. On peut s'attendre à des résultats défavorables de l'interprétation des chaînes de caractères spécifiques de contrôle Baudot (par exemple des chaînes parasites BT ou EOT).

Par conséquent, la transformation (filtrage) de la sortie binaire est nécessaire aux systèmes de communication qui sont sensibles aux fonctions de commande ou aux chaînes de caractères de commande. Des exemples de diverses techniques de filtrage sont décrits dans l'annexe B. L'annexe C présente une comparaison des effets des différents filtres décrits dans la présente partie de l'ISO 10126.

6.2 Absence de filtrage

Lorsque le service de transmission est transparent aux caractères et aux chaînes de commande, il n'est pas nécessaire d'utiliser un filtre de transmission. Toutefois, si les séparateurs explicites comme décrit en 5.3.1.2 sont utilisés, il est important d'éviter la présence de ces séparateurs dans le cryptogramme (voir 6.9).

6.3 Filtrage hexadécimal

Le filtrage doit être effectué en convertissant chaque quartet du cryptogramme en un caractère hexadécimal, puis en le transmettant dans le code de caractères utilisé par le réseau. L'exemple 1 de l'annexe B décrit un filtre hexadécimal.

6.4 Filtre ISO 646

Les réseaux utilisant le code de caractères conformément à l'ISO 646 (Version internationale de référence) et qui ne transforment pas en majuscules les lettres en minuscules peuvent utiliser le filtre à 94 caractères décrit ici. L'exemple 2 de l'annexe B décrit un filtre ISO 646 (IRV).

Le flot binaire est divisé en groupes d'unités de données de 13 bits, chaque unité de données étant considérée comme un entier binaire non signé. La dernière unité de données doit être complétée jusqu'à 13 bits si nécessaire (voir 6.6). Les deux caractères correspondant au nombre à 13 bits se trouvent au tableau 1. Le décodage s'effectue en inversant le processus.

Un seul tableau suffit pour ce filtre (le tableau 1 présente les 95 premières valeurs de ce tableau). La première colonne comprend les nombres de 0 à 8 191 en ordre. La colonne 2 convertit cette entrée d'origine en l'une des 8 192 premières paires possibles de caractères imprimables autres que le blanc et le trait d'union figurant dans l'ISO 646, tableau 11, Version internationale de référence, en ordre lexicographique.

Le premier caractère de cette paire de caractères sous forme filtrée peut être représenté différemment dans l'ISO 646 si modifié pour une utilisation nationale. Toutefois, la présente partie de l'ISO 10126 utilise ces éléments seulement comme véhicules pour transformer les vecteurs à 13 bits en vecteurs à 14 bits et ne requiert pas l'impression des caractères. C'est pourquoi, aucun conflit ne résulte de l'utilisation de diverses représentations nationales.

Tableau 1 — Filtre ISO 646 (Présentation de la séquence des caractères permis)

Entrée originale	Format du filtre		Entrée originale	Format du filtre		Entrée originale	Format du filtre	
0	!	!	14	!	0	29	!	?
1	!	"	15	!	1	30	!	@
2	!	#	16	!	2	31	!	A
3	!	¤	17	!	3	32	!	B
4	!	%	18	!	4	33	!	C
5	!	&	19	!	5	34	!	D
6	!	'	20	!	6	35	!	E
7	!	(	21	!	7	36	!	F
8	!	)	22	!	8	37	!	G
9	!	*	23	!	9	38	!	H
10	!	+	24	!	:	39	!	I
11	!	,	25	!	;	40	!	J
12	!	-	26	!	<	41	!	K
13	!	/	27	!	=	42	!	L
			28	!	>	43	!	M

Entrée originale	Format du filtre		Entrée originale	Format du filtre		Entrée originale	Format du filtre	
44	!	N	62	!	'	80	!	r
45	!	O	63	!	a	81	!	s
46	!	P	64	!	b	82	!	t
47	!	Q	65	!	c	83	!	u
48	!	R	66	!	d	84	!	v
49	!	S	67	!	e	85	!	w
50	!	T	68	!	f	86	!	x
51	!	U	69	!	g	87	!	y
52	!	V	70	!	h	88	!	z
53	!	W	71	!	i	89	!	{
54	!	X	72	!	j	90	!	|
55	!	Y	73	!	k	91	!	}
56	!	Z	74	!	l	92	!	~
57	!	[	75	!	m	93	"	!
58	!	\	76	!	n	94	"	"
59	!	]	77	!	o	95	"	#
60	!	^	78	!	p	⩔		
61	!	_	79	!	q	8 191	z	(