INTERNATIONAL STANDARD

ISO 9160

First edition
1988-02-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ORGANISATION INTERNATIONALE DE NORMALISATION
МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ

Information processing — Data encipherment — Physical layer interoperability requirements

Traitement de l'information — Chiffrement de données — Caractéristique interfonctionnement dans la couche physique

Reference number
ISO 9160 : 1988 (E)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work.

Draft International Standards adopted by the technical committees are circulated to the member bodies for approval before their acceptance as International Standards by the ISO Council. They are approved in accordance with ISO procedures requiring at least 75 % approval by the member bodies voting.

International Standard ISO 9160 was prepared by Technical Committee ISO/TC 97, *Information processing systems*.

Users should note that all International Standards undergo revision from time to time and that any reference made herein to any other International Standard implies its latest edition, unless otherwise stated.

Printed in Switzerland

Information processing — Data encipherment — Physical layer interoperability requirements

0 Introduction

This International Standard specifies interoperability and security related requirements for using encipherment at the physical layer of the ISO Open Systems Interconnection (OSI) Reference Model in telecommunication systems conveying Automatic Data Processing (ADP) information.

This International Standard will facilitate the interoperation of data encipherment equipment used in data communication facilities and systems that require cryptographic protection.

The objectives of physical layer encipherment are to protect against all forms of passive attack including traffic analysis. Full protection against traffic analysis can only be provided in synchronous operation where all bits can be enciphered, whereas in asynchronous operation the start and stop bits can never be enciphered. This International Standard does not provide for protection of physical connection establishment.

This International Standard contains two annexes, A and B. Annex A is not an integral part of this International Standard. Annex B is an integral part of this International Standard.

1 Scope and field of application

This International Standard applies to systems for encipherment of ADP information in the physical layer of data communications.

This International Standard is equally applicable whether the Data Encipherment Equipment (DEE) is implemented as a physically separate piece of equipment or implemented as part of the Data Terminal Equipment (DTE) or as part of the Data Circuit terminating Equipment (DCE). When the encipherment is integrated into the DTE or DCE, this International Standard applies to those portions of the DTE or DCE design which implement the requirements of this International Standard. Interoperability requirements are defined for the following physical interface definitions: V.24, X.20 bis, X.21 bis, X.20, and X.21.

The physical layer is described in the Open Systems Interconnection Reference Model, ISO 7498. In physical layer encipherment, all of the SDU is normally enciphered. The interoperability requirements described in this International Standard apply to both synchronous and asynchronous operation in both full duplex and half duplex modes.

The main body of this International Standard specifies requirements which are applicable to the use of various encipherment algorithms. Annex B specifies additional requirements for the use of DEA (ANSI X3.92 – 1981).

This International Standard also specifies two alternative modes of synchronous operation – the delayed option and the immediate option – which are mutually incompatible.

This International Standard also specifies two alternative actions for BREAK signalling for asynchronous operation – Class A and Class B – which are mutually incompatible.

2 References

The following documents are referenced in this International Standard:

ISO 2382 – 9, *Data Processing – Vocabulary – Part 9: Data Communication.*
ISO 7498, *Information processing systems – Open Systems Interconnection – Basic Reference Model.*
ISO 7498 – 2, *Information processing systems – Open Systems Interconnection – Basic Reference Model. Part 2: Security Architecture*[1)]
ISO 8372, *Information processing – Modes of operation for a 64 – bit block cipher algorithm*
ANSI X3.92 – 1981, *Data Encryption Algorithm.*
CCITT, *Recommendations X.20, X.20bis, X.21, X.21bis – Red Book VIII.3 – 1984.*
CCITT, *Recommendations V.24, V.54 – Red Book VIII.1 – 1984*

3 Definitions

3.1 This International Standard makes use of the following data communication terms defined in ISO 2382 – 9:

1) At present at the stage of draft; publication anticipated in due course.

Physical layer	Serial transmission
Data communication	Asynchronous transmission
DTE	Start Stop transmission
DCE	Start signal
DCE/DTE Interface	Stop singal
Call establishment	Synchronous transmission
Data transfer	Duplex transmission
Test loops	Half duplex transmision

3.2 This International Standard makes use of the following terms drawn from the respective International Standards.

Service Data Unit (SDU)	(ISO 7498)
Physical connection	(ISO 7498)
Ciphertext	(ISO 7498/2)
Plaintext	(ISO 7498/2)
Initializing Value (IV)	(ISO 8372)
Starting Variable (SV)	(ISO 8372)

4 Applicable interfaces

Where an interface exists between the DEE and the DTE, DCE, or with both, this interface may be one of those recommended by CCITT such as V.24, X.20, X.20bis, X.21 or X.21bis. This International Standard refers to the call establishment of a physical layer connection which is signalled in a different manner across these different interfaces. Control signals not affecting, nor affected by, DEE operation shall be passed through or re-driven at the DEE.

A DEE presenting a standard DCE/DTE Interface needs to delay some control signals such, as 'Ready for Sending', 'Data Set Ready', or the 'Ready for Data' indications, when relaying them to the DTE, as required to complete its own operations.

The delay caused by the DEE, together with the delay caused by the DCE, shall fit into the time-out requirements determined by the DTE. The DTE shall not commence data transmission prior to having received the appropriate control signal as mentioned above.

4.1 V.24 Interfaces

For interchange circuits to Recommendation V.24, circuit 108 ('Data Terminal Ready' / 'Connect Data Set to Line') from the DTE to the DCE, if used by the DCE, circuit 107 ('Data Set Ready') from the DCE to the DTE, and circuit 109 ('Data Channel Received Line Signal Detector') from the DCE to the DTE are always passed through or redriven with minimal delay by the DEE.

However, it is recommended that the DEE delays the ON condition on circuit 109 to the DTE until such time as the DEE is in a position to deliver data to the DTE on circuit 104 ('Received Data'). The DEE shall not signal the ON condition on circuit 109 to the DTE until after the ON condition on circuit 107 has been signalled to the DTE.

Inserting a DEE into a DTE/DCE Interface introduces inherent delays in control signals and should consider the time-out provisions of existing equipment. The time-outs depend, among other things, on duplex transmission and half duplex transmission. The appropriate modem recommendation should be consulted.

4.1.1 Duplex Transmission

Call establishment of a physical connection is indicated by reception by the DEE of the ON condition on circuit 107 from the DCE. In leased line operation, circuit 107 is permanently ON. Both the transmit and receive data channels are active at the time circuit 109 and circuit 106 are ON.

The DEE shall not signal the ON condition on circuit 106 to the DTE until such time as all of the following conditions are met:
a) Circuit 107 is switched ON from the DCE to the DEE and passed through by the DEE to the DTE
b) Circuit 105 from the DTE, if required by the DCE, is switched ON and passed through to the DCE.
c) Circuit 106 from the DCE is ON and the initiating DEE operations are completed.

A physical connection can be cleared by:
a) the DCE, indicated by the transition to the OFF condition of circuit 107, as a national option; or by
b) the DTE, indicated by the transition to the OFF condition of circuit 108; or by
c) the DEE, indicated by the transition to the OFF condition of circuit 108 to the DCE and of circuit 107 to the DTE. When this happens it indicates a fault condition in the DEE.

4.1.2 Half-Duplex Transmission

Call establishment of a physical connection is indicated by reception of the ON condition on circuit 107 from the DCE. In leased line operation circuit 107 is permanently ON. Depending on the condition of the 'Request to Send' (circuit 105), either the transmit or receive data channel is active at a time.

The ready for sending state, circuit 106 ON, is indicated by the DCE after the DTE and the DEE switched circuit 105 ON. The ready for receiving state is indicated by the ON condition of circuit 109 from the DCE.

Circuit 105 is used such that the transition to the ON condition is always passed through or re-driven with minimal delay by the DEE. The transition to the OFF condition to the DCE is delayed by the DEE until the last data bit is transmitted on 'Transmitted Data' (circuit 103). Circuit 106 ON from the DEE to the DTE is indicated after initiating DEE operations are completed.

A physical connection can be cleared by:
a) the DCE, indicated by the transition to the OFF condition of circuit 107, as a national option; or by
b) the DTE, indicated by the transition to the OFF condition of circuit 108; or by
c) the DEE, indicated by the transition to the OFF condition of circuit 108 to the DCE and of circuit 107 to the

DTE. When this happens it indicates a fault condition in the DEE.

NOTE – To avoid false DEE decipherment starts, caused by false signals on circuit 104 which can occur shortly after the ON to OFF transition on circuit 105 and the following OFF to ON transition on circuit 109 in the DCE, the DEE should be used with a DCE which uses the clamping option of V.24, clause 4.3, together with the longer OFF to ON response time of circuit 106 as specified in the relevant DCE recommendation.

4.2 X.20bis or X.21bis Interfaces

For interchange circuits to CCITT Recommendations X.20bis and X.21bis consult the applicable V.24 operation for duplex transmission as described above.

4.3 X.20 Interfaces

For interchange circuits to CCITT Recommendation X.20, Call establishment of a physical connection provides for start–stop and duplex transmission. It is indicated by reception of the call control character ACK on the 'Receive' interchange circuit R. In leased circuit service, data can be transmitted and received at any time.

In circuit switched service, reception of data (ready for receiving state) may take place immediately after reception of ACK. This state is called 'Connected'. Transmission of data (ready for sending state) may take place not earlier than 20 ms after ACK. This later is called 'Ready for Data'.

The 'Connected' state from the DEE to the DTE is indicated by ACK after the initiating DEE operations are completed.

Clearing of a physical connection is indicated by the 'DCE clear confirmation' at the clearing DTE or the 'DTE clear confirmation' at the cleared DTE, both indicated by the transmission of continuous binary zeros on circuit R, i.e. r = O, which persists for at least 210 ms. Clearing may be initiated either by 'DTE clear request' from the DTE, 'DCE clear indication' from the DCE, or by the DEE indicating 'DTE clear request' to the DCE and 'DCE clear indication' to the DTE. The DEE initiated disconnect indicates a fault condition in the DEE.

4.4 X.21 Interfaces

For interchange circuits to CCITT Recommendation X.21, call establishment of a physical connection provides for synchronous and duplex transmission. It requires the 'Transmit' interchange circuit T from the DTE to the DCE in ON condition. Call establishment is indicated by the 'Ready for Data' state, which is the transition to ON on the 'Indication' interchange circuit I from the DCE. In leased circuit service, circuit I goes ON as a response to circuit T switched ON. Circuit T from the DTE to the DCE is always passed through or re–driven with minimal delay by the DEE.

The transmission and reception of data (ready for sending state and ready for receiving state) may take place not earlier than 16 bit times after i = ON.

The 'Ready for Data' state, i.e., i = ON, from the DEE to the DTE is indicated after the initiating DEE operations are completed.

Clearing of a physical connection is indicated by the 'DCE clear confirmation' at the clearing DTE or the 'DTE clear confirmation' at the cleared DTE, both indicated by a transition to OFF on circuit I from the DCE together with binary zeros on circuit R, i.e., r = 0, i = OFF. Clearing may be initiated either by 'DTE clear request' from the DTE, 'DCE clear indication' from the DCE, or by the DEE indicating 'DTE clear request' to the DCE and 'DCE clear indication' to the DTE. The DEE initiated disconnect indicates a fault condition in the DEE.

4.5 Transmitted and Received Data Interchange Circuits

The term 'transmitted data interchange circuit' in this International Standard refers, in the case of a V.24, X.20bis or X.21bis interface, to circuit 103 and in the case of an X.20 or X.21 interface to circuit T.

The term 'received data interchange circuit' in this International Standard refers, in the case of a V.24, X.20bis or X.21bis interface, to circuit 104, and in the case of an X.20 or X.21 interface to circuit R.

5 General requirements

When employing this International Standard for interworking between DEEs, the following conditions are required in all DEEs of an interworking group:

a. The same cipher algorithm.
b. The same cryptographic key value.
c. The same IV length, IV structure, and IV bit transmission order.

This International Standard does not specify a particular cipher algorithm but does require any algorithm used to be applicable on a single bit or single character at a time basis, as appropriate to the physical layer service provided.

NOTES

1. The use of a block cipher algorithm in the 1–bit cipher feedback (CFB–1) mode of operation specified in ISO 8372 meets the requirements of this International Standard.
2. Annex B contains the IV requirements when the DEA (ANSI X3.92–1981) algorithm is used for encipherment.

If there is loss of synchronization between DEEs and this condition is detected, resynchronization can be forced by the DEE or DTE, by clearing the physical connection, followed by the re–establishment of the physical connection using procedures appropriate to the type of interface as specified in clause 4. The DEE shall not initiate connection re–establishment.

6 Synchronous encipherment operation

6.1 IV

The IV length and IV structure may be chosen according to the application. There shall be prior agreement concerning IV length and IV structure among all the DEEs in an interworking group.

6.2 Transmission

Upon call establishment of a physical connection and indication of the ready for sending state, the transmitted data interchange circuit is in a MARK condition. The IV is sent at this point in time, preceded by a single binary zero bit to delimit the IV. Encipherment continues until clearing of the physical connection or data channel turn – around in half duplex transmission.

The transmission of the first enciphered data bit of the SDU shall follow the transmission of the IV according to one of the following alternatives.

6.2.1 Alternative A: Immediate

The first enciphered data bit follows immediately after transmission of the IV.

6.2.2 Alternative B: Delayed

Immediately following transmission of the IV, an indeterminate number of binary one bits (MARK condition) may be transmitted. However, if this alternative is used this delay condition shall be maintained for a minimum of 10 ms, up to a maximum of 50 ms. The binary one bits are followed by a single binary zero bit to delimit the data, followed by the first enciphered data bit.

6.3 Reception

Upon call establishment of a physical connection and indication of the ready for receiving state, the received data interchange circuit is in a MARK condition. The IV is received immediately following the first binary zero bit. In Alternative A, all subsequent received bits are then deciphered. In Alternative B, the receiving DEE shall be capable of recognising the delimiting binary zero bit and deciphering incoming data within 10 ms. In both Alternative A and Alternative B, decipherment continues until clearing of the physical connection or data channel turn – around in half duplex transmission.

Figure 1 shows the operation of the V.24 interchange circuits for duplex transmission. Figures 2 and 3 illustrate the V.24 half duplex transmission signalling sequences for synchronous encipherment Alternative A and B respectively.

7 Asynchronous encipherment operation

NOTE – The use of a physical connection capable of duplex transmission is recommended in order to improve the efficiency of operation.

7.1 Transmission

7.1.1 IV

Upon the establishment of a physical layer connection and indication of the ready for sending state, the transmitted data interchange circuit is in a MARK condition. The IV shall be sent subdivided into units equal to the size of the characters about to be enciphered and transmitted. The IV length and IV structure may be chosen according to the application. There shall be prior agreement between transmitting and receiving DEE on IV length, IV structure, and framing of the IV in transmitted characters.

7.1.2 Starting Encipherment

Characters of the SDU (corresponding to characters on the transmitted data interchange circuit), framed within start and stop signals, are transmitted enciphered following the last IV character. Start and stop framing signals are not enciphered. Encipherment continues, except for BREAK (described below), until clearing of the physical connection or data channel turn – around in half duplex transmission. Figure 4 illustrates the start of asynchronous encipherment as well as the Class A BREAK operation described below.

7.1.3 BREAK

BREAK is signalled by a SPACE condition existing for one character time or longer. The action of the DEE on a BREAK shall be according to one of the following alternatives.

7.1.3.1 Class A

The first binary zero bit of the BREAK is treated as a start signal. The next n binary zero bits are enciphered, where n is the normal character length in bits without the start signal snd stop signal. The stop signal (MARK condition) is not output by the DEE. Subsequent binary zero bits in the BREAK are not enciphered and the DEE continues to output the binary zero state. Figure 4 illustrates this action on the right hand side. The transition to the MARK condition at the DEE input produces a corresponding transition at the DEE output. Subsequently, the DEE resumes its normal operation.

7.1.3.2 Class B

The DEE normally does not output any character until the stop signal has been received. BREAK is detected by the absence of the expected stop signal. Having detected a BREAK the DEE outputs an identical BREAK, suspending encipherment. The end of the BREAK is output after a suitable delay, following which normal operation is resumed. Figure 5 illustrates Class B break operation.

7.2 Reception

7.2.1 Starting Decipherment

Upon call establishment of a physical connection and indication of the ready for receiving state, the received data interchange circuit is in the MARK condition. In accordance with the agreement between transmitting and receiving DEE on IV length, IV structure and its framing in characters, the first characters received, exclusive of start signal and stop signal, are considered as the IV. All

subsequent characters, exclusive of start signal and stop signal, are deciphered. Decipherment continues, except during BREAK, until clearing of the physical connection or data channel turn – around in half duplex transmission.

7.2.2 Reception of BREAK

The action of the DEE receiving the enciphered form of the BREAK depends on the class of operation of the transmitting DEE, as follows.

7.2.2.1 Class A

The character comprising enciphered binary zero bits is deciphered. The absence of the stop signal indicates that a BREAK operation has begun. The receiving DEE output holds the SPACE condition until the BREAK ends at the DEE input, after which it outputs the transition to the MARK condition and resumes normal operation. Figure 4 illustrates this operation on the right hand side.

7.2.2.2 Class B

The BREAK is detected by the absence of the stop signal. The DEE does not output any character until the stop signal has been received. Having detected a BREAK it outputs an identical BREAK, suspending decipherment. The end of the BREAK is output after a suitable delay, following which normal operation is resumed. Figure 5 illustrates this operation.

8 Bypass control facility (Optional)

As an additional capability, physical layer encipherment may optionally provide a bypass of the encipherment process for test loop operation under control of interchange circuits as described in CCITT Recommendations V.54, X.20bis, and X.21bis. In this International Standard it is not specified for the X.20 and X21 interfaces, although the test loops are defined as user facilities of the interface.

When this option is used, bypass occurs whenever circuit 142, 'Test Indicator' from the DCE, is ON, and either circuit 141, 'Local Loopback', or circuit 140, 'Loopback/ Maintenance Test' from the DTE, is ON. Both circuit 140 and circuit 141 simultaneously ON is considered an error condition and bypass mode is not entered. The DEE re – signals either loopback signal over the interface to the DCE and re – signals 'Test Mode' to the DTE. Figure 6 illustrates the operation of these circuits with the local or remote loopback of data.

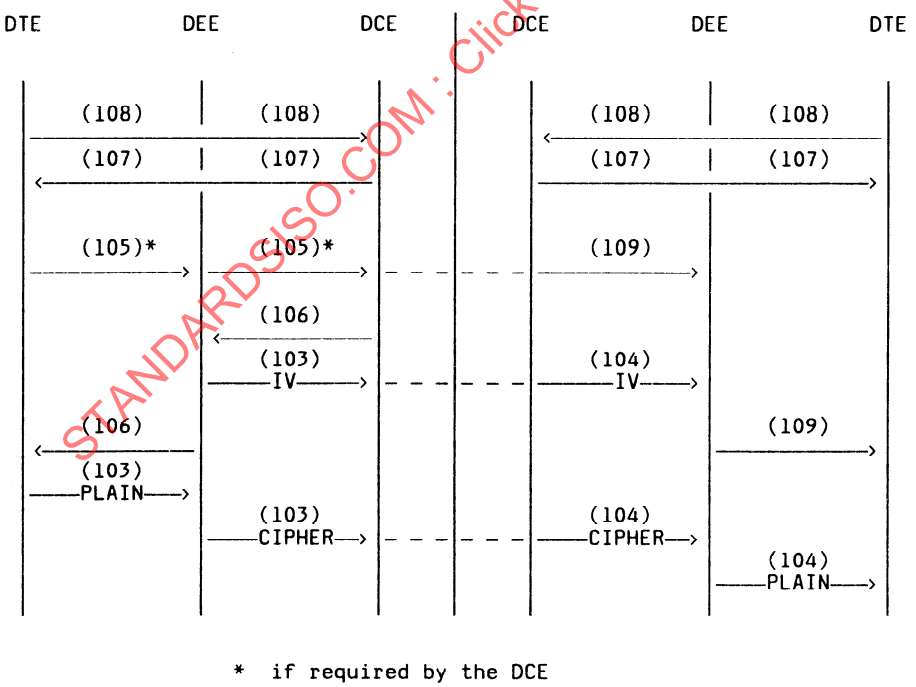


Figure 1 — Operation of the V.24 Interchange circuits showing data encipherment in one direction only

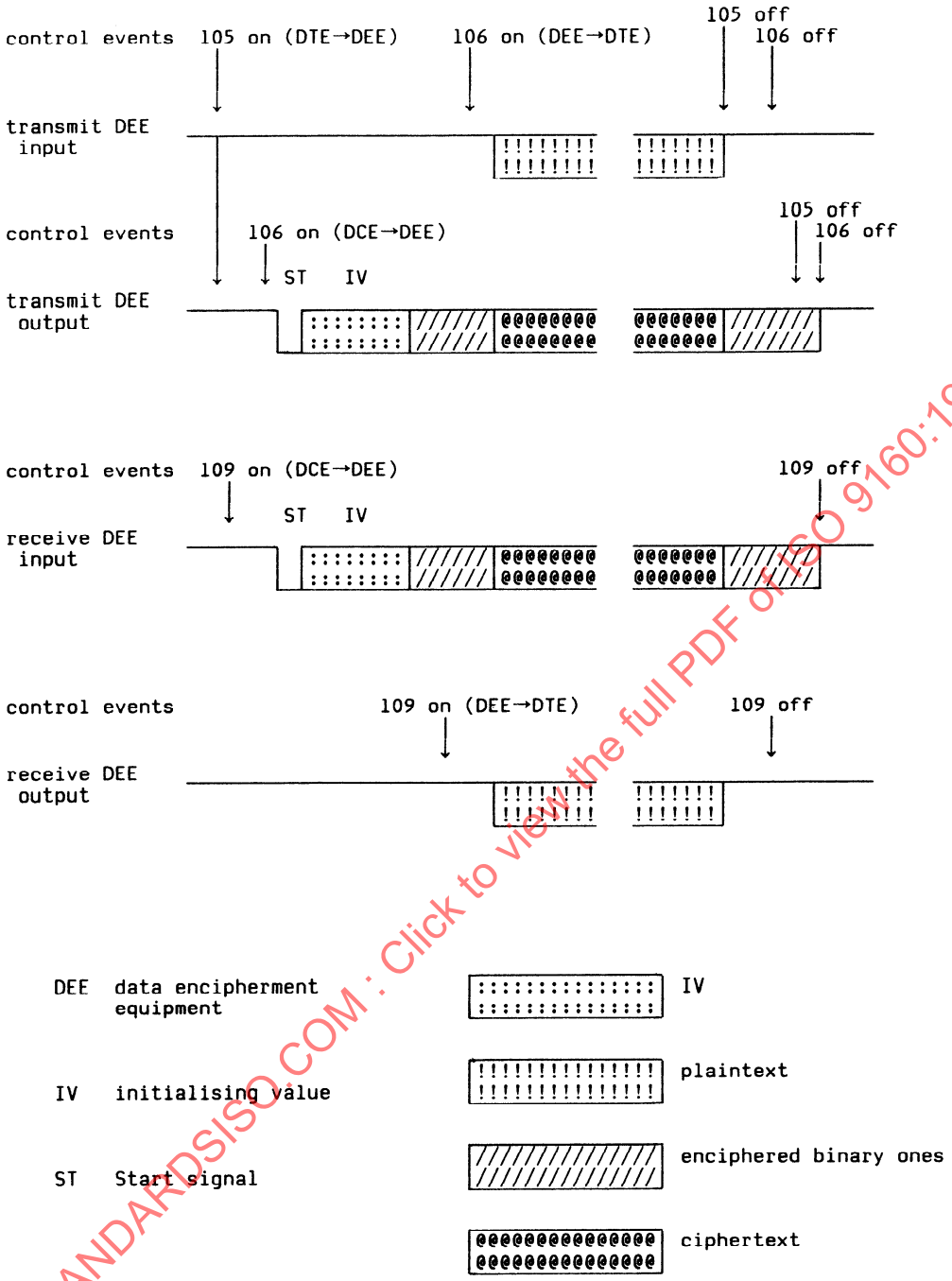


Figure 2 — V.24 Half Duplex Transmission Signalling Sequence for Synchronous Encipherment, Alternative A

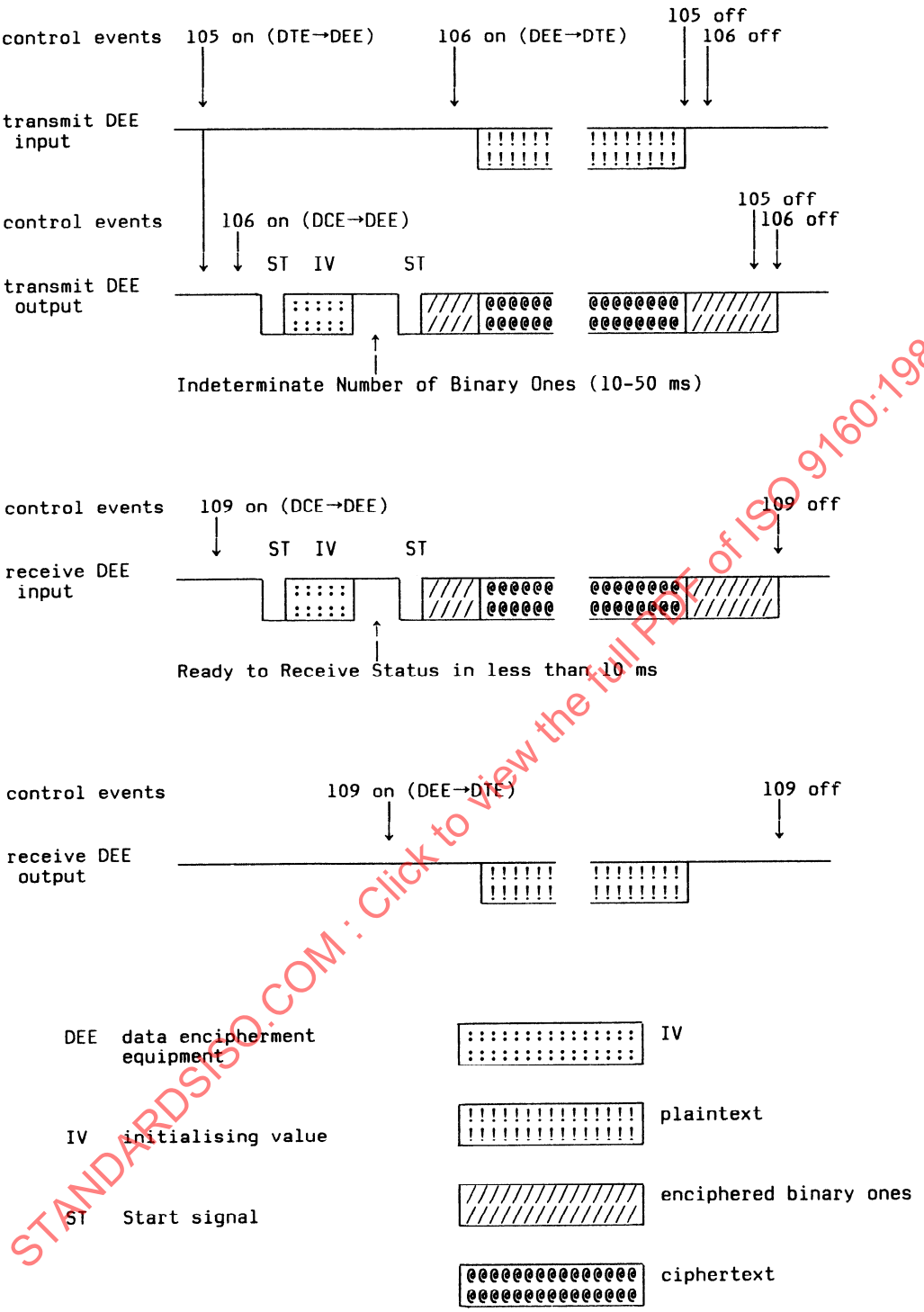


Figure 3 — V.24 Half Duplex Transmission Signalling Sequence for Synchronous Encipherment, Alternative B

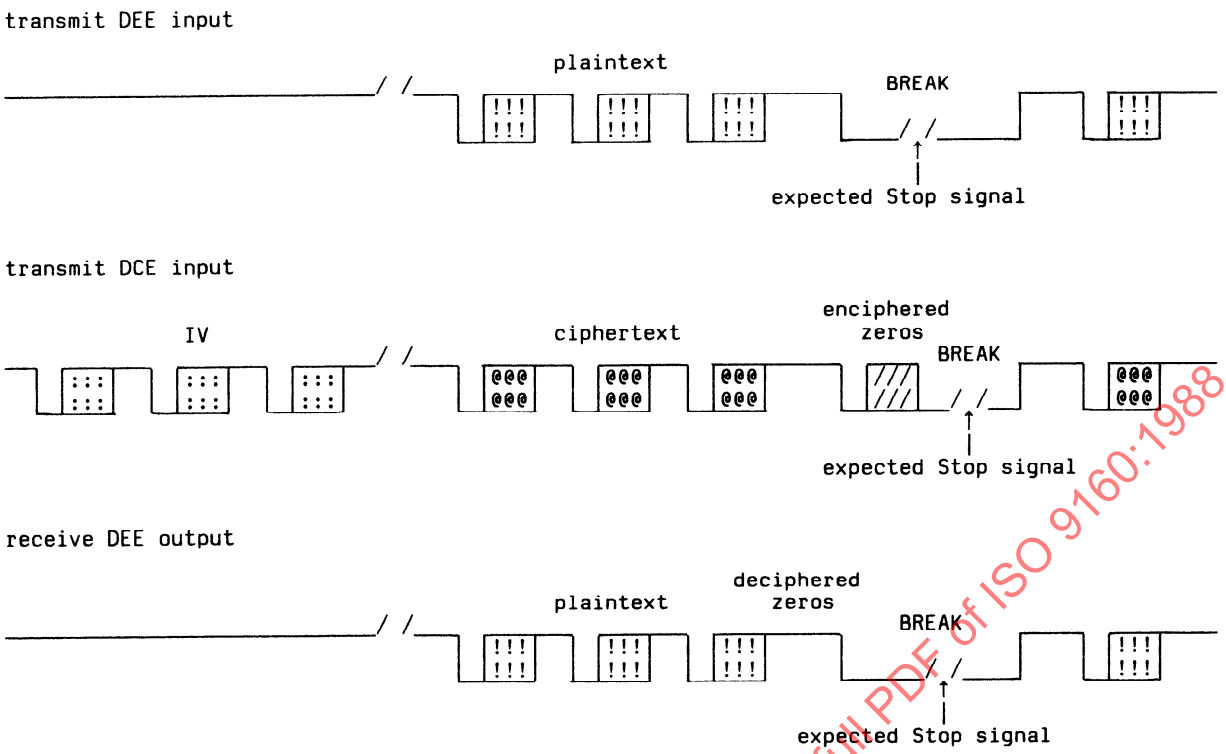
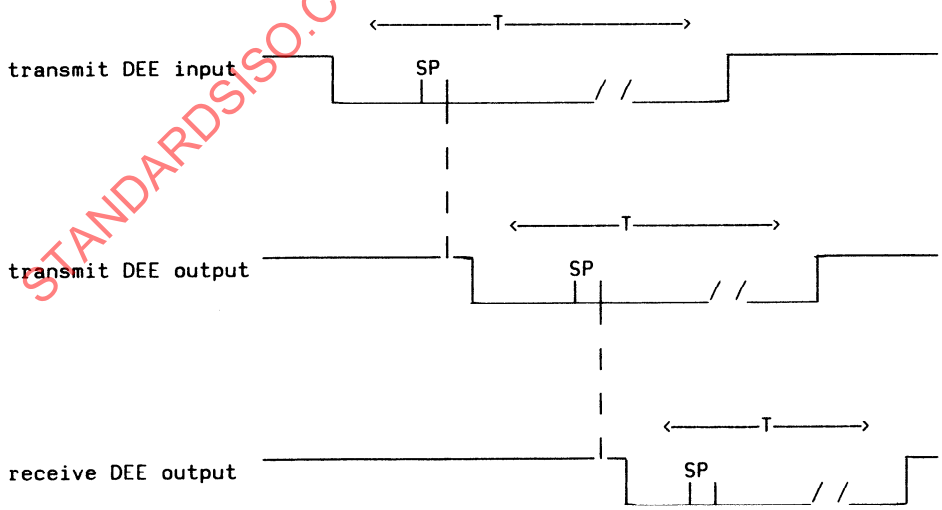


Figure 4 — Start of asynchronous encipherment and a Class A BREAK operation



SP = Expected Stop Signal

Figure 5 — Class B BREAK operation

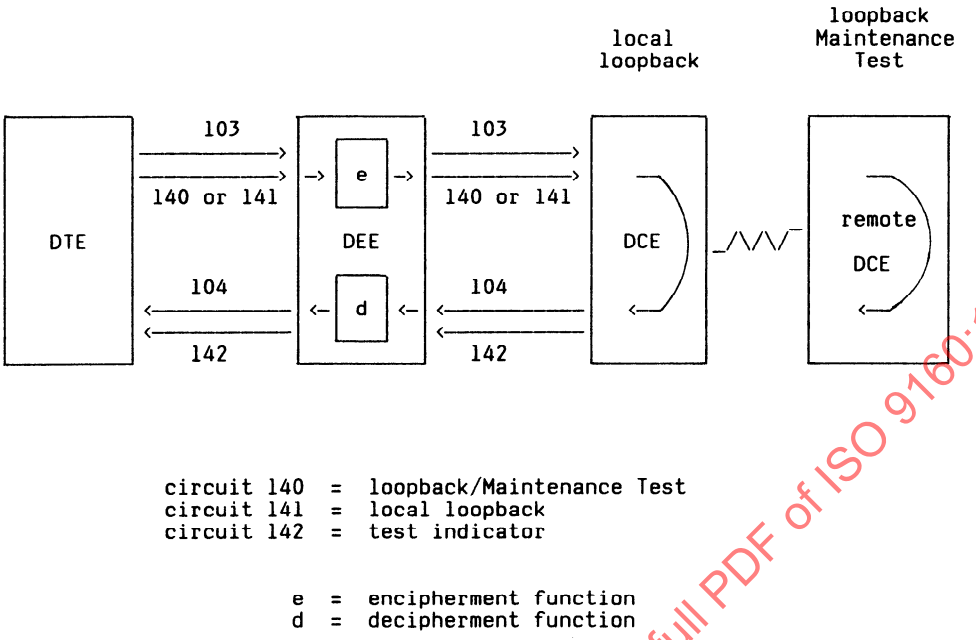


Figure 6 — Bypass of encipherment for Test Loop Operation

Annex A

Background Information on Encipherment in the Physical Layer

(This Annex is not an integral part of this International Standard.)

A.1 Characteristics of encipherment in the Physical Layer

Encipherment in the physical layer can allow the DEE to be of simple design. It usually requires no change to link or higher layer procedures or protocols.

The use of a block cipher in the CFB – 1 mode could restrict the data rate if the implementation of encipherment operations were limiting factors. However, physical layer encipherment is often used at relatively low data rates.

The changes to the performance of the link that may be perceptible to higher layers are:
a. The delay after call establishment of a physical connection and indication of the ready for sending and receiving state before data passes due to sending of the IV, and the traffic overhead. This is important only in the case of rapid data channel turn – around in half – duplex transmission with short messages. With full duplex operation it may be of no practical importance.
b. The extension of transmission errors. A single bit error in the ciphertext will cause, in general, errors extending over several bits in the received plaintext. Error control procedures must be able to deal with such bursts, or may need to be altered to match this error property. Encipherment in the physical layer conceals the content of all SDU information on the line, including all higher layer headers and addresses. This concealment of traffic information may be useful.

No procedures are provided in physical layer encipherment for detection of insertion, deletion, modification or replay of data. Protection against such 'active attack' threats can be provided only at higher layers.

A.2 Alternatives Provided in the International Standard

Alternatives are provided for action on a BREAK in asynchronous operation (Classes A and B).

Class A BREAK operation operates on a bit – by – bit basis. It delays data through the DEE by only a little more than one bit time. It however generates a character without a proper Stop signal, which may not be acceptable to all communication channels, in that it may result in a data error indication in addition to a BREAK. Class B BREAK operation requires a data delay of at least one START/ STOP transmission time. DEE for asynchronous operation may provide one or both classes of break operation.

A.3 Bypass Control Facility (optional)

Bypass is intended to facilitate diagnosis of line – faults by local and remote modem loopback. It is not necessary to provide for bypass at both (or all) ends of a connection. The bypass facility in a DEE does not effect its compatibility with other DEEs not having this option.

The presence of a bypass facility could, in some circumstances, weaken security. Users should consider this factor, as well as the convenience of automatic line testing. If necessary a DEE could be fitted with a control of bypass, allowing it to be put out of action when not needed, and brought into action when needed.

If such a switch is provided it is recommended that it be under the control of a physical key in a lock. It may provide one or more of the following three modes of operation as selectable alternatives:

A.3.1 Bypass mode

When physically enabled, the DEE is effectively transparent to the data transmission path. Encipherment and decipherment procedures in the DEE are bypassed for all data. SDUs appear in plaintext at the DEE – DCE interface.

A.3.2 Bypass/Secure mode

When physically enabled, bypass would be controlled by the loopback and test indicator signals. That is, the DEE provides bypass capability only during automatic line testing. Hence when this mode is selected, bypass would occur only when circuit 142 from the DCE is ON along with either circuit 141 or circuit 140 from the DTE (see Figure 6).

A.3.3 Secure Mode

Provides the capability to transfer only ciphertext user data across the DEE – DCE interface.

Annex B

Requirements for IV Structure and Transmission for DEA (ANSI X3.92 – 1981)

(This Annex is an integral part of this International Standard.)

B.1 General

The optional IV lengths provide greater security but for many users the security of the mandatory IV is sufficient. If the IV delay and overhead is significant, there will be a motive for the mandatory IV. This is a tradeoff for the user to make. DEE may provide options with a switchable choice.

B.2 Synchronous Encipherment Operation

The DEE shall support an IV length of 48 bits. In order to produce the 64 – bit SV from the IV, 16 zeros are concatenated on the left. Following these zeros, the next bit of SV is the first bit of IV transmitted.

The DEE may optionally support an IV length of 64 bits. The SV equals the IV, with the first transmitted bit on the left.

B.3 Asynchronous Encipherment Operation

The DEE shall support an IV length which is the lowest integer multiple of the character size equal to or greater than 48 bits (see Table 1). In order to produce the 64 – bit SV from the IV, binary zero bits are concatenated on the left. Figure 7 illustrates the derivation of the SV for 7 – bit characters with an IV of 49 bits.

Table 1 : IV Derivation

bits per character	5	6	7	8
characters per IV	10	8	7	6
size of IV	50	48	49	48

B.3.1 IV Option 1

The DEE may optionally support an IV length which is the lowest integer multiple of the character size equal to or greater than 60 bits (see Table 2). In order to produce the 64 – bit SV from the IV, binary zero bits are concatenated on the left. Figure 8 illustrates the derivation of the SV for 7 – bit characters with an IV of 63 bits.

Table 2 : IV Option 1

bits per character	5	6	7	8
characters per IV	12	10	9	8
size of IV	60	60	63	64

B.3.2 IV Option 2

The DEE may optionally support an IV length which is the lowest integer multiple of the character size equal to or greater than 64 bits (see Table 3). In order to produce the 64 – bit SV from the IV, bits transmitted beyond the 64 are discarded, the first bits transmitted being those discarded if this is necessary. Figure 9 illustrates the derivation of the SV for 7 – bit characters with an IV of 70 bits.

Table 3 : IV Option 2

bits per character	5	6	7	8
characters per IV	13	11	10	8
size of IV	65	66	70	64

B.4 Recommended Classification of Options (Optional)

The following terminology should be used to define the options described in this International Standard and Annex as implemented in particular equipment.

B.4.1 Synchronous Encipherment Operation

Field	Contents	Description
1	S	Synchronous encipherment operation
2.1	IV	Initialising Value
2.2	(blank)	Mandatory length (48 bits)
	1	Mandatory and optional (48 and 64 bits)
3.1	T	Transmission
3.2	1	Alternative A: immediate
	2	Alternative B: delayed
4	(blank)	No bypass facility
	BP	Bypass facility provided

B.4.2 Asynchronous Encipherment Operation

Field	Contents	Description
1	A	Asynchronous encipherment operation
2.1	IV	Initialising Value
2.2	(blank)	Mandatory length
	1	Mandatory and option 1
	2	Mandatory and option 2
3.1	B	Break operation
3.2	1	Class A
	2	Class B
4	(blank)	No bypass facility
	BP	Bypass facility provided

B.4.3 Examples

Examples of compliance level definitions are:

S – IV – T2 – BP A – IV1 – T2 A – IV – B1 A – IV2 – B2 – BP

or when there is equipment with multiple possibilities:

A – IV12 – T12 – BP S – IV1 – B12 A – IV1 – T12 S – IV12 – B1 – BP

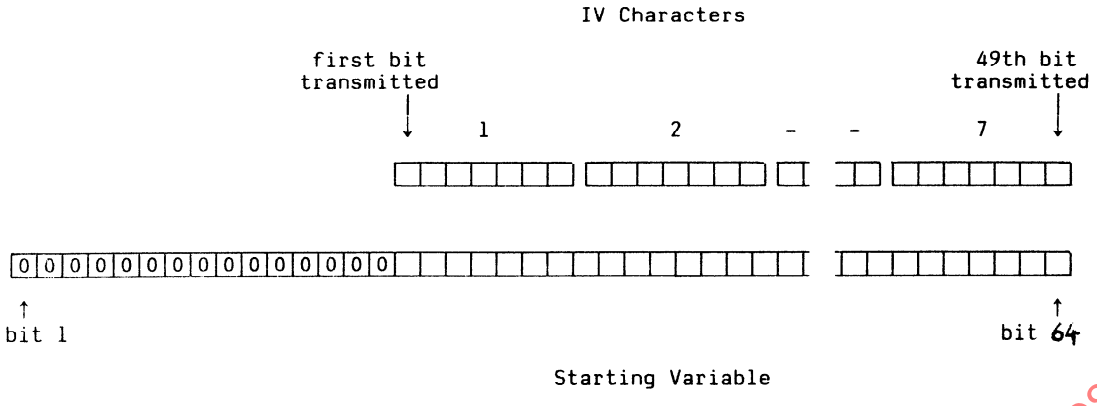


Figure 7 — SV Derivation from 49-bit IV, 7-bit Characters, Preferred Alternative

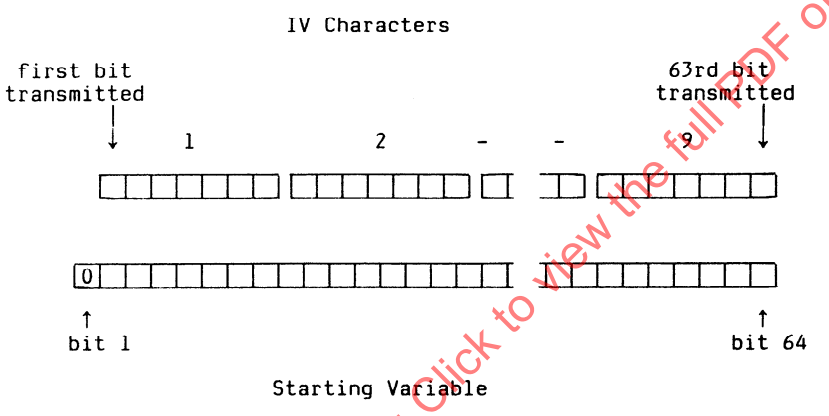


Figure 8 — SV Derivation from 63-bit IV, 7-bit Characters, Acceptable Alternative 1

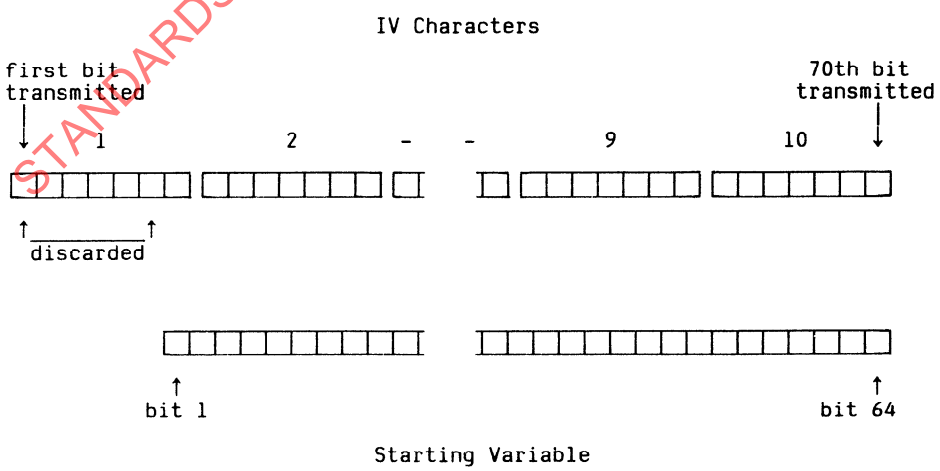


Figure 9 — SV Derivation from 70-bit IV, 7-bit Characters, Acceptable Alternative 2