Monograph:

Clark, John Andrew orcid.org/0000-0002-9230-9739 and Jacob, Jeremy Lawrence orcid.org/0000-0003-4806-7426 (1997) A survey of authentication protocol literature: Version 1.0. Report. Citeseer

1 **5**
1.1 B . . . 5
1.2 A P R . . . 6

2 **7**
2.1 G P . . . 7
2.2 S K C . . . 7
2.2.1 C C . . . 8
2.2.2 M C . . . 8
2.2.3 M B C U . . . 9
2.2.4 S C . . . 12
2.3 P K C . . . 13
2.4 O - H A . . . 15
2.5 N C . . . 16

3 **17**
3.1 S K T T P . . . 17
3.2 S K T T P . . . 18
3.3 P K . . . 20
3.4 H P . . . 22
3.5 O F P . . . 22
3.6 G . . . 22

4 **23**
4.1 F A . . . 23
4.2 T F . . . 23
4.3 P S A . . . 26
4.4 I D A . . . 28
4.4.1 S C . . . 29
4.4.2 C B C . . . 29
4.5 B A . . . 33
4.6 E A . . . 34
4.7 O F A . . . 35
4.8 C . . . 36

5 **37**
5.1 E F S . . . 37
5.2 T U L . . . 39
5.2.1 BAN L . . . 39

5.2.2 O L 41
5.3 E S A R S 42

6 **44**
6.1 S K P T T P . . . 44
6.1.1 ISO S K O -P U A -
P 44
6.1.2 ISO S K T -P U A -
P 44
6.1.3 ISO S K T -P M A 44
6.1.4 ISO S K T -P M A 45
6.1.5 U N -R F 45
6.1.6 A S RPC P 45
6.2 A U C C F 46
6.2.1 ISO O -P U A CCF . 46
6.2.2 ISO T -P U A CCF . 46
6.2.3 ISO T -P M A CCF . . . 46
6.2.4 ISO T -P M A CCF . . 46
6.3 S K P I T T P . . 46
6.3.1 N S P C K 46
6.3.2 D S P 47
6.3.3 O -R P 47
6.3.4 A N S P 48
6.3.5 M F P 48
6.3.6 49
6.3.7 C S K I P 50
6.3.8 ISO F -P A P 50
6.3.9 ISO F -P A P 50
6.3.10 L A P 50
6.3.11 L M A 53
6.4 S C K E 54
6.4.1 N -S S P 54
6.5 S K R A 55
6.5.1 K 5 55
6.5.2 N S 57
6.5.3 K L S 58
6.5.4 T K C R A P . 58
6.6 P K P T T P 59
6.6.1 ISO P K O -P U A
P 59

6.6.2 ISO P K T -P U A P 59
6.6.3 ISO P K T -P M A P - 59
6.6.4 ISO T -P M A P . . . 60
6.6.5 ISO T P P M A P 60
6.6.6 B K E P K 60
6.6.7 D H E 60
6.7 P K P T T P 61
6.7.1 N -S P K P 61
6.8 SPLICE/AS A P 61
6.8.1 H C M SPLICE/AS 62
6.9 D S K D P K 63
6.9.1 CCITT .509 63
6.10 M 64
6.10.1 S R A T P 64
6.10.2 G M A P 64
6.10.3 E K E EKE 65
6.10.4 D S P K C 66

7 **67**

1.1

T

, -

. T -

. T , ;

.

P ,

. T -

. L ,

.

( )

.

A -

26 . A

; ,

( ) -

. T

, , -

-

.

A -

. T , ,

-

. T N S C K P -

1978 87

. I 1981, D S

42 . T -

. T -

(2). I 1994 M

A D S

1 . I 1995, L

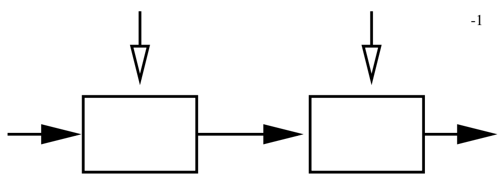
N
S ( ). I
(
).
T
. I ,
. T
. S , -
- . I
-
. A . S
.

1.2

A ! T
. H , -
. H ,
" " -
. T
(, , , -
.)

2.1

C .
S
. . A
-
. T .
T . T
C
.
T *C* -
. T , .
T . E
1.



F 1: E D

T -
. B
.

2.2

I
. U -
.
T
. O ,

. T
. F -
A *B*
.

2.2.1

C . T -
( )
. A
. A
. T
. E , , -
-
(. . N
). E
. I -
. T 41, 99 . A
114 .

2.2.2

M
.
A (64 128)
. T D E -
S 45 , DES. T
. T
(56 128
N S A)
- (113),
- (-
). T 101 . I
- - -

B S 1988. A C 1994 38
DES
1974! O ,
.

O MADR GA (
8-), NE DES (64-
120-), FEAL-N, RC2 RC4 (R
R) IDEA (L M). S
IDEA 98 . A -
( ) S
99 .

2.2.3

T . P
:

E C B (ECB)

C B C (CBC)

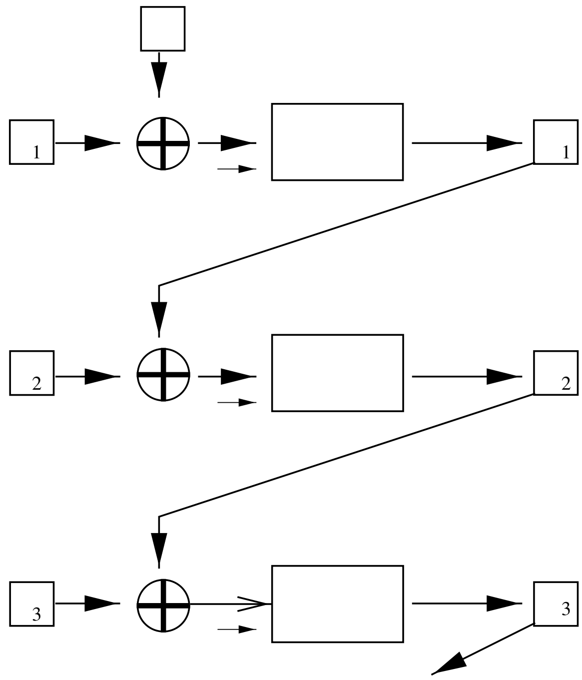
C F M (CFB)

O F M (OFB)

ECB . C
. T , -
( ). I
. A
- (
). A ,
(. .
).
C B C (CBC)
. I
D E S (DES)
. B - (OR)
1
.
F ,
E(:)

E(:) C C C C

C
0 C (: (C))



F 2: C B C

H , (:) . T -
2.
S -
(:)

0 C (: C)

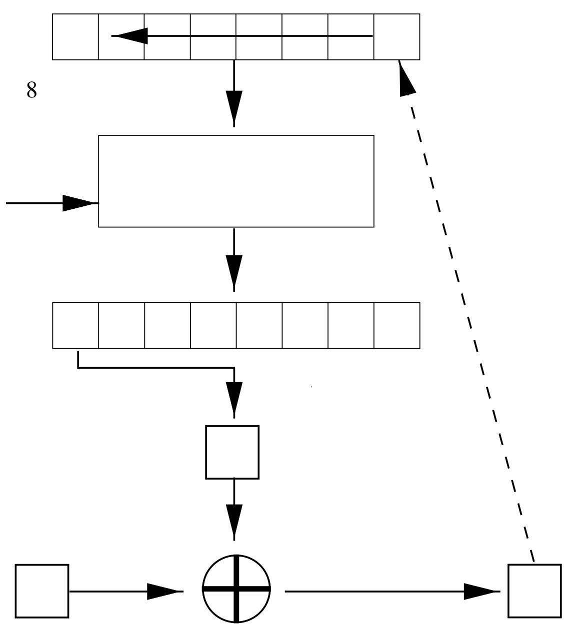
T , -
( ).
I
. I -
- -
(-
). A

(S 99) (
D P 39). K 112
- CBC.
T -
. F S

. C
J 36 ;
,

!
I , -
(. . -
-). I C
F (CFB) . F 3
S 99 8- CFB 64- . H
. T
,
OR .
T 8 -

. T .

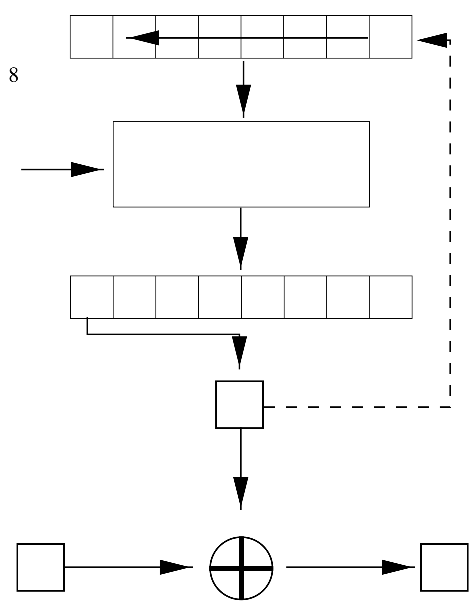


F 3: C F M

O F (OFB) 4. H ,

( ).

S CFB OFB
, -
99 . K 1 12 .
T
. T S 99
D P 39 .
O , . . C (OFB
, . .),
B C (OR
) P -
C B C (
OR
). T
; .

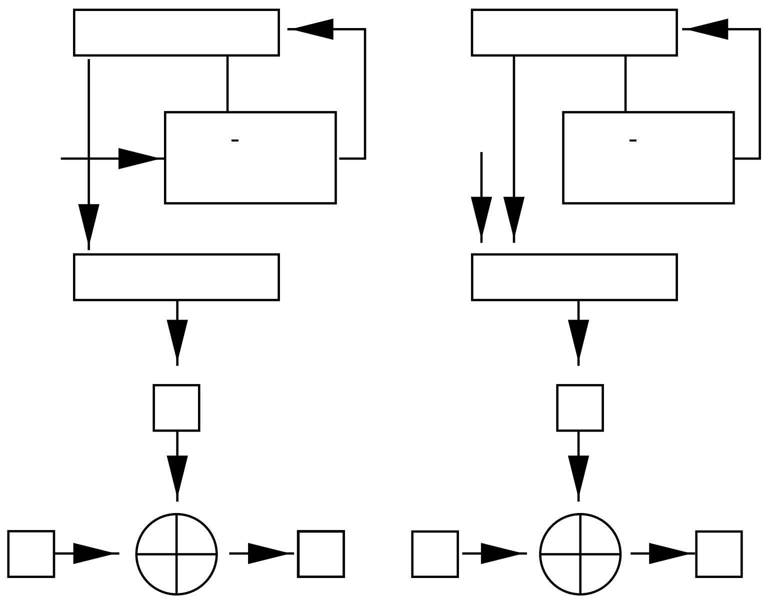


F 4: O F M

2.2.4

S . T
OR

. C -
. I , -
(99). T
(
). A
. F 5 -



F 5: S C A

- : (
)
; C (-
,).
I (. .
C M).
F S 99 .

2.3

I -
. T
D M H 1976 44 . I

A ( ). T
A -
. A
A . T ,
A .
S

. I C ( )

A . T
. T
R , S A 92 -
RSA. S
. S
.
(G 49).
T RSA 92 :

1. ,

2. ( ) (1)(1)

3. E 1 ( )

4. ( ) . T
.

5. C .

6. C C .

H (-
).
A A B

B . B
A .
P ( )
(. .
D H RSA). A ,
. C
. F , 512

RSA ; 512 -
(1024). S
. P -
.
S 99 .

T (
) . H -

58 . 115 . G 56 -
. D
43
. B O -
( ) 25 . O
M
81 .

2.4 -

. T
. A H M
H(M) .
H(M) . T
- ; M H(M) -
M H(M)=H(M). T
. A
.
H -
.

I *A* *B*
, , *E*(: ( ))
M
. O , *B* ( )
E(: ( ))
. S
(*A* *B*
).

2.5

I *E*(:)

.

A

. P

A, *B* ( ). T

(1) *A* *B* :

(2) *B* :

(3) *B* :

A *B*, *B*

B. A

.

. T (*A*) *A*.

-

A

A ( ).

A *A* . S

.

- . S

, , ISO (61).

A ;

. M -

. T

(1) *A* *B* : *A* *E*(:)

A *B* -

A -

E(:).

I -

. A

, . .

. (

)

. T

: (. . -

, - , - .) -

(-)

(-

). T ISO

(61).

3.1

P ( ) ISO

O - S K U A P 62 (

6.1.1) . I :

(1) *A* *B* : 2 *E*(: *B* 1)

H ;

( ).

A (. .) -

(. .

). T

-

. O ,

B, *A*,

A

. N -

((1),

B , *B*).

T - -

- . O *A* -

B. *B*

A -

. F 6 - . I

. I ,
,
B . *A*
B -
. *A*
B (
).

(:)

F 6: A C R P

T - . S -
, ; ,
( ). G -
53 .

T ISO T -P U A P
(6.1.2). T ISO T - T -P M A -
P 6.1.3 6.1.4 .
A
. E ,
. E
6.2. E P 4 ISO
64 .

3.2

S (TTP)
. T ,
N S S K A 87

:

(1) *A* : *A* *B*
(2) *A* : *E*(: *B* *E*(: *A*))
(3) *A* *B* : *E*(: *A*)
(4) *B* *A* : *E*(:)
(5) *A* *B* : *E*(: 1)

I *A*
B. H
. T *A* (2)
. (2). O *A*
. I

. *A* *B* *E*(: *A*)
(3).
P *B*
A. H ,
( ), *A*
(4).
P *A*, , ,
1, *B* (5). *B* -
. T
B *A* (3
).
A ,

. R ,
. 4.1
.
T
: A
N -S P 88 (6.3.4), P (
6.3.6), O -R P 91 (6.3.3)
A N -S P . L
116, 117 (6.3.10). O -
G C
( ) (6.10.2 6.3.7) ISO F - F
P M A P 62 (6.3.8 6.3.9).
D S N
S . T D S C

K P N S
:

(1) A : A B
(2) A : $E($: B $E($: A $))$
(3) A B : $E($: A $)$

H , . A B
(2) (3) (. .
).

T
. C M F P B -
( ) 26 :

(1) A : A $E($: B $)$
(2) B : $E($: A $)$

A . O (1)
" " , ,
B . B (2)
.
H (
). D S
40 .

S . T
- . T A -
B. T

B . I A
B ;
( ). T
. S K 68
N S 90 .

3.3

P

-
; , S RSA 100
DES (

RSA 64 K). H -

, -

-

.

N S -

87 :

(1) *A* : *A* *B*
(2) *A* : *E*(: *B*)
(3) *A* *B* : *E*(: *A*)
(4) *B* : *B* *A*
(5) *B* : *E*(: *A*)
(6) *B* *A* : *E*(:)
(7) *A* *B* : *E*(:)

H , ,

,

.

T

. M (1), (2) (5), (6) *A* *B*

. M (3) *B*

B. I

A . *B* ,

A

(6). *A*

(6). S *B*

A *B*

. *A* *B* B

(7). *B*

A

. T ( )

74 .

S , -

D SP (S 99 L 117). T

CCITT .509 29 -

. T ISO -

.

D S -

42 . M A 1994

1 .

P -

. RSA 92

. I -
. T
. A RSA ,
, U S N S A
(NSA) D S A . I E G -
. S 99
A
2 . O ESIGN, M E (
). A
3 .

3.4

T -
. A (-
) E K E (EKE) B M 15 .
T -
. I
.

3.5

T . F , -
- , , -
, . T S
99 . E
61 , 62 , 63 , 64 , 65 . R
S 66
H 57 . L 73 -
( ).

3.6

T -
. S
100 . A
9 . T
8 , 7 .

I
.

4.1

A ( )

. T -
N S
( ) 3.2.
A ,

. T
. I 1981, D S
42 . C (3). A *B*
(-)
,
. T ,
(, -
) .

(3) $E($: $A)$. H *B*
( ):

(3) (A) B : $E($: $A)$
(4) B (A) : $E($: $)$
(5) (A) B : $E($: $1)$

B . -
(5) . H
B
A. D S
42 . T
88 .

4.2

A (
, , ,

). T .
A

.
F , A S RPC P

(1) A B : A $E($: $)$
(2) B A : $E($: 1 $)$
(3) A B : $E($: 1$)$
(4) B A : $E($: $)$

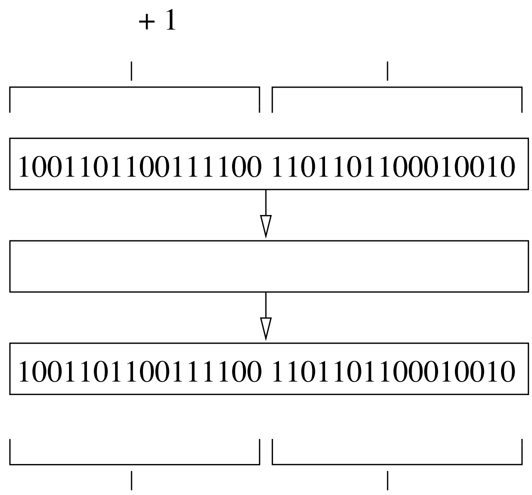
H , A B
$E($: $)$ (1). B

$E($: 1). A B
$E($: 1) B. B
( )
.
H ,
, 64 , (2),
(3) (2) (4). T
:

(1) A B : A $E($: $)$
(2) B A : $E($: 1 $)$
(3) A (B) : $E($: 1$)$
(4) (B) A : $E($: 1 $)$

T A 1
. T
7.
T -

. F , ,
. T . I
A
.
T . F ,
(4)
, . . , B ,
A N 26 .



F 7: B S I T F

T O -R 91
.

(1) *A* *B* : *A* *B* *E*(: *A* *B*)
(2) *B* : *A* *B* *E*(: *A* *B*) *E*(: *A* *B*)
(3) *B* : *E*(:) *E*(:)
(4) *B* *A* : *E*(:)

T
A *B*. .
A *A* (4)
(1)
. I ( ) 32 , *A* *B* 16
64
(1) (4). T

(1) *A* (*B*) : *A* *B* *E*(: *A* *B*)
(4) (*B*) *A* : *E*(: *A* *B*)

H *A* *E*(: *A* *B*)
(M,A,B) . M, A B

( ). S , -
(3) (4)
(2) *B*. T :

(1) *A* *B* : *A* *B* *E*(: *A* *B*)
(2) *B* ( ) : *A* *B* *E*(: *A* *B*) *E*(: *A* *B*)
(3) ( ) *B* : *E*(: *A* *B*) *E*(: *A* *B*)
(4) *B* *A* : *E*(: *A* *B*)

H *A* *B*
(*A* *B*).
F S 109 H
60 .

4.3

A -

.
A -
:

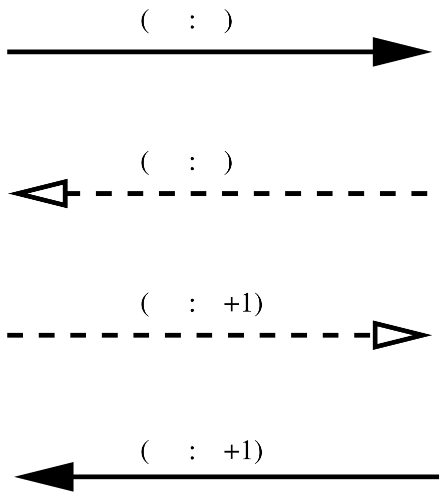
(1) *A* *B* : *E*(:)
(2) *B* *A* : *E*(: 1)

S *A* *B*
B
(1). I ,
.
I , *B* .
T
.

(1 1) *A* (*B*) : *E*(:)
(2 1) (*B*) *A* : *E*(:)
(2 2) *A* (*B*) : *E*(: 1)
(1 2) (*B*) *A* : *E*(: 1)

H *A* (1.1).
B (2.1),
(1.1). *A*
(2.2). B *A*

. (1.2). A
A *B* . I , *B* . T
8. S
, .



F 8: S P S A

I *A* .
H
" " *A*
. *A* (
) .
A -M
F P ( ). T -
B , A N 26 .

(1) *A* : *A* *E*(: *B*)
(2) *B* : *E*(: *A*)

H , (*A* *B*)
. I *A* *B*
(1) .
O (1) " "
, , *B* . *B*
(2)
( ).
T -
-

. I -
B (. .

) .
T

- A B.

(1) A : A E(: B)
(2) B : E(: A)
(1) (B) : B E(: A)
(2) (A) : E(: B)
(1) (A) : A E(: B)
(2) (B) : E(: A)

A
B . H A B
.
P 103, 117, 108, 60 . B
18, 19 -
.

4.4

C 31
. T -
-

( ). F
. T ,

-

.
S 4.2
( ) . I

.
P ( )
-
. I

. T
( )
.

4.4.1

A - - . T
,
.
C N S
3.2.

(4) *B* *A* : *E*(:)
(5) *A* *B* : *E*(: 1)

S (4) . N
(
) 1 1 . O
, (5)
. O
.
T B 21 . I
. A

. F ,

( ).
I
A. M (3)
:

(3) *A* *B* : *E*(: *A*)

F *A* *C*
. S *A* *B*
C *C*.

4.4.2

A C B C -
2.2.3. F
(

). S *E*(:) *C C C* T *C C C*
C ,
. S *C C* (*C*)
C C .
T

. T

.
C (2) N S -
4.1.

(2) *A* : *E*(: *B* *E*(: *A*))

S *C C C C*
. T *E*(: *B*) *C C C* . B
A (3) *B*
. T ,
. T CBC
.
S G 106

(
). T
9.

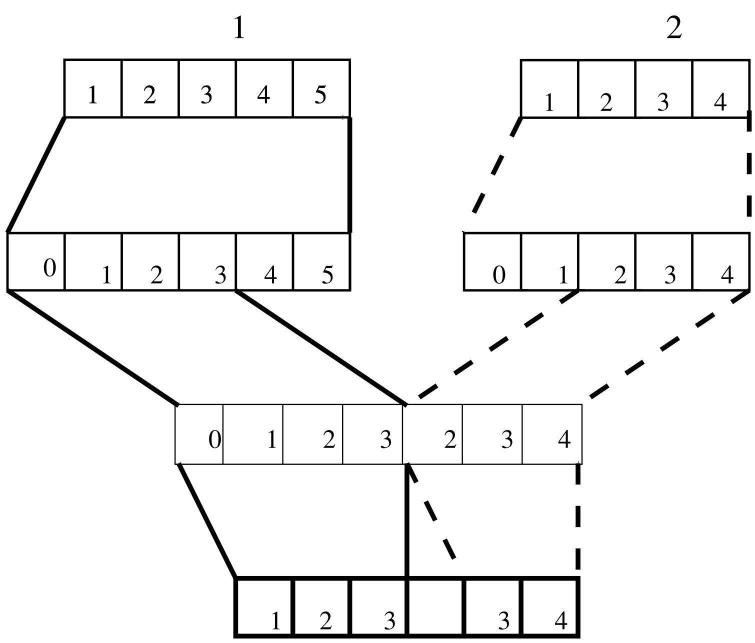
. D
,
(. .
). M B
CBC 79 , -

-
. I 9,

C (*C*)

C (*C*)

.
I
;



3 ⊕ (2)

F 9: S A C B C

( ).
O -
C . C
C C .
T

C (C)

N

OR 0. A (
)

(C (C))

C (C)

C C C C
. I
. T
.
A ,
(2) N S . (2)
A B. I
(2) (
)
. T , . N
(3) :

(3) A B : E(: A)

S A (3), (3)
. O A

: B
(3) . T .
N S -
. T
.

.
T . I ,
. I -
, P C B C (PCBC)
K .5 CBC (.4
PCBC). C K B
M 14 . O C B C
B 13 .

4.5

I .
S . T
. P

. T ,

.
T ,
;
. I ,
. C :

(1) *C* *A* : *C*
(2) *A* *C* : *A* *E*(: *A* *C*)

H , *C*
. T *A* -
. *C* (1) . H
.
A (2). T *A*
C .
T -
A ,
C .
H ,
(2)
. T :

(1 1) *C* (*A*) : *C*
(2 1) (*C*) *A* : *C*
(2 2) *A* (*C*) : *A* *E*(: *A* *C*)
(1 2) (*A*) *C* : *A* *E*(: *A* *C*)

H *C* *A* -

A 2.1. *A* , *C* -
, (2.2).
C (1.2). *C*
. T
( ) H C 59 . T

(2). T :

(1) *C* *A* : *C*
(2) *A* *C* : *A* *E*(: *A* *C*)

P
CCITT .509 . L A M 12
B , A N 26 (
6.9.1).

4.6

I *A* -
B *A*. A
-
. A
D S 40 :

(1) *B* *A* : *E*(: *A*)
(2) *A* : *E*(: *A*) *B*
(3) *A* : *E*(: *B*)

I .
T . *A* (3) *B*
. T -
(
). H , *C*
(3) (1) *A*
C. S *B*
. C ? G -
. I
,
(CRC) . I CBC

( ).
N ,
. T 3
( )
3 CBC -
. S
(
).

4.7

T -
. I ,
.
M -
J M 85 .
I ,
. M B 80 -
. P K
RSA -
72 .
A G 51 . P -
15 , 54 .
C 31
. T ( ) CCITT .509
(-
BAN) N 89
. I -
. C J -
CCITT .509 -
34 . A N
10, 11 . A -
5 .

4.8

P ;
. T , ,

.
T
-
.
A ,
! A L 76
.
T , ,
. T -

. A
5 . A N -
-
1 .
T (-
) . T
.

I
. S ,
. :
-
;
;
- .

T R H 95 -
. A R H ,
.
T
.
H , -
:
.

5.1

E -
. T ; -
(,
G) -
. T ,
,
.
T K , 1987
I J
69 . T -
. E ,
. T .
T , ,
.
B M -
24 . N . T

-
. UK
G . D . M -
, B 17 .
T .
T - . T
(K -
, M B). T
. -
. S
-
.
O -
, . . LOTOS .509
. F -
. N
. R
H 95 .
R F S E P R -
G O 94
. I
CSP. P CSP -
. I ,
(, ,
.)
A (
).
T -
. T F -
D R (FDR)
. R G
.
T (
). F ,
17 N S
P K L FDR 75 . S 77 . R
G
94 . T -
47 48 . A

-
( ). F CSP
S -
97 . A CSP
R 96 .

5.2

L -
. T :

(,);

(,).

T ,
. S
107
. H

. T -

.

5.2.1

I 1989, B , A N
26 . T
(*BA*) -
. T
. T
. T ,

.
BAN ;
-
. I ,

.
T . N 89 -
-
BAN . E ,

. S -
,
. I 27 BAN
,
.
T , .
A . S 102
.
I
. F -
.
G , N 55
(GN) . A , -
BAN
(
BAN). GN
. GN
. T ,
. M BAN
. , -
(. .
). T
G 52
.
B M 24 BAN (
): ;
(. .
) . I
. A R H 95
. T
(BAN),
.
T - . B M -
- (. .
) 24 . C 30
BAN
. T -

. L

.

K BAN

71 . T . T

- BAN .

A

,

. A

( )

. K

. B

( )

,

(. . N -

). T BAN

. R B M

23 O

120 .

O , BAN . I

. T R N (

GN). K BAN

BAN , . BAN

-

( ) . I

. T T BAN ;

. T -

; . BAN

; -

. S

.

A BAN

. I .

5.2.2

G ( )

. B 16

CKT5 KT5 (-

) . C

32

CKT5 . S
B - ,
. . .
H B -
. S
. S
HOL (H O L) -

104 .

5.3

T
. E M -
I 84 . T
83 . P -
. K
. T , ,

, . .
. T
. I
70 . T

(,
103). A

T , ,
, .
, -
.

S - .
S 104 I -
- . BAN .
A I -
.
M (
NRL P A). T -

. P
. R
.
.
(. .
). T
. T -
R H 95
. I ,
TMN
RSA 70 . T
; .

6.1

6.1.1 -

T 62 *A*
B. A
.

(1) *A* *B* : 2 *E*(: *B* 1)

T . T
N T
.

6.1.2 -

I *A* *B*
- . T :

(1) *B* *A* : 1
(2) *A* *B* : 3 *E*(: *B* 2)

H . O (2) *B* -
B
(1). A *B* *A* -
((2) (*B*)
(1)).

6.1.3 -

T
. A ,
A *B*.

(1) *A* *B* : 2 *E*(: *B* 1)
(2) *B* *A* : 4 *E*(: *A* 3)

T - -
(6.1.1). U
.
A ,
-
.

6.1.4 -

H

.

(1) *B* *A* : 1
(2) *A* *B* : 3 *E*(: *B* 2)
(2) *B* *A* : 5 *E*(: 4)

O (2) *B* *B*
(1). O (3) *A*
(1) (2) .

6.1.5 -

I , -
. O (2) *B*
( ) . H -

A,
.

(1) *B* *A* : *B*
(2) *A* *B* : *A* *E*(: ( ) *A*)
(3) *B* *A* : *B* *E*(: ( ))

6.1.6

T . I
A *B*. I (4)
.

(1) *A* *B* : *A* *E*(:)
(2) *B* *A* : *E*(: 1)
(3) *A* *B* : *E*(: 1)
(4) *B* *A* : *E*(:)

T (4)
A . A
A (. .
B). T .

6.2

A ISO P 4 ISO 9798
S 64 . T ( )
.

6.2.1 -

(1) *A* *B* : *B* 2 (*B* 1)

6.2.2 -

(1) *B* *A* : 1
(2) *A* *B* : 3 (*B* 2)

6.2.3 -

(1) *A* *B* : 2 (*B* 1)
(2) *B* *A* : 4 (*A* 3)

T -
.

6.2.4 -

(1) *B* *A* : 1
(2) *A* *B* : 3 (*B* 2)
(3) *B* *A* : 5 (4)

6.3 -

6.3.1

T (-) S P . T
87 (*1*). T
.

(1) *A* : *A* *B*
(2) *A* : *E*(: *B* *E*(: *A*))
(3) *A* *B* : *E*(: *A*)
(4) *B* *A* : *E*(:)
(5) *A* *B* : *E*(: 1)

T D S 42 . T

.

T *B*

(3) . A

(3) *B* .

A , *A* ( ) (3)

(*B*).

I

(4) (5) ( )

. T 21 . S 4.4.1.

6.3.2

D S N

S . T :

(1) *A* : *A B*

(2) *A* : *E*(: *B* *E*(: *A*))

(3) *A* *B* : *E*(: *A*)

. *B* (3) (

). T -

A *B* N -S .

6.3.3 -

T O -R P 91 -

. T

26 .

(1) *A* *B* : *A B E*(: *A B*)

(2) *B* : *A B E*(: *A B*) *E*(: *A B*)

(3) *B* : *E*(:) *E*(:)

(4) *B* *A* : *E*(:)

I ( ). I (1) *A* *B*

A B

. *B*

. T

A B . I

, (3) *B*

A. *A* *B*

.
A :

(1) A (B) : A B E(: A B)
(4) (B) A : E(: A B)

I A A B . T . T . O , (2) - A B .

6.3.4

I 1987 N S 88 N - S P . T .

(1) A B : A
(2) B A : E(: A)
(3) A : A B E(: A)
(4) A : E(: B E(: A))
(5) A B : E(: A)
(6) B A : E(:)
(7) A B : E(: 1)

T (- ; B 21).

6.3.5

T 26 . I B .

(1) A : A E(: B)
(2) B : E(: A)

A . O (1) " " , , B . B (2) . T ( ).

T -
- -
.
T

- *A* *B*.

(1) *A* : *A* *E*(: *B*)
(2) *B* : *E*(: *A*)
(1) (*B*) : *B* *E*(: *A*)
(2) (*A*) : *E*(: *B*)
(1) (*A*) : *A* *E*(: *B*)
(2) (*B*) : *E*(: *A*)

A *B*

(1) *A* ( ) : *E*(: *B*)
(2) ( ) *B* : *E*(: *A*)

T .

6.3.6

T . I
. T
C J
( ).

(1) *A* *B* : *A*
(2) *B* : *B* *E*(: *A*)
(3) *A* : *E*(: *B*) *E*(: *A*)
(4) *A* *B* : *E*(: *A*) *E*(:)

O :

(1) (*A*) *B* : *A*
(2) *B* ( ) : *B* *E*(: *A*)
(3) :
(4) (*A*) *B* : *E*(: *A*) *E*(:)

O . A
108 .

6.3.7

T - 33 .

(1) *A* *B* : *A*
(2) *B* : *A* *B*
(3) *B* : *E*(: *A*) *E*(: *B*)
(4) *B* *A* : *E*(: *B*) *E*(:)
(5) *A* *B* : *E*(:)

6.3.8 -

(1) *A* *B* : *B* 1
(2) *A* : 4 *E*(: *B* 3) *E*(: *A* 2)
(3) *A* *B* : 6 *E*(: *A* 2) *E*(: *B* 5)
(4) *B* *A* : 8 *E*(: *A* 7)

6.3.9 -

(1) *A* *B* : 1
(2) *B* : *A* 2
(3) *B* : 5 *E*(: *A* 4) *E*(: *B* 3)
(4) *B* *A* : 7 *E*(: *B* 3) *E*(: 6)
(5) *A* *B* : 9 *E*(: 8)

6.3.10

T - . S
. T
117 . L

" ,
".

L
. T . N : 1994
117 L
.

T .

(1) A B : A
(2) B A :
(3) A B : $E($ $: A$ B $)$
(4) B : $E($ $: A$ B $E($ $: A$ B $))$
(5) B : $E($ $: A$ B $)$

T .

(1) A B : A
(2) B A :
(3) A B : $E($ $: A$ B $)$
(4) B : $E($ $: A$ B $E($ $: A$ B $))$
(5) B : $E($ $: A$ B $)$

T .

(1) A B : A
(2) B A :
(3) A B : $E($ $: A$ $)$
(4) B : $E($ $: A$ $E($ $: A$ $))$
(5) B : $E($ $: A$ $)$

T .

(1) A B : A
(2) B A :
(3) A B : $E($ $:$ $)$
(4) B : $E($ $: A$ $E($ $:$ $))$
(5) B : $E($ $: A$ $)$

T .

(1) A B : A
(2) B A :
(3) A B : $E($ $:$ $)$
(4) B : $E($ $: A$ $E($ $:$ $))$
(5) B : $E($ $:$ $)$

T :

(1) (*A*) *B* : *A*
(2) *B* (*A*) :
(3) (*A*) *B* :
(4) *B* ( ) : *E*(: *A*)
(1) *B* ( ) : *B*
(2) ( ) *B* : *E*(:)
(3) *B* ( ) : *E*(: *E*(:))
(4) (*B*) : *E*(: *E*(:))
(5) (*B*) : *E*(:)
(5) ( ) *B* : *E*(:)

H *B* (1)
.

A :

(1) (*A*) *B* : *A*
(1) *B* :
(2) *B* (*A*) :
(2) *B* :
(3) (*A*) *B* :
(3) *B* : *E*(:)
(4) *B* : *E*(: *A*)
(4) *B* : *E*(: *E*(:))
(5)
(5) *B* : *E*(:)

T 117 . H , -
.
F ,

(1) (*A*) *B* : *A*
(2) *B* (*A*) :
(3) (*A*) *B* :
(4) *B* ( ) : *E*(: *A*)
(5) ( ) *B* : *E*(: *A*)

S .
L -
. E (
, L 76)

-

. T , L

. T . I

:

(1) *B* : *B*
(2 1) (*A*) *B* : *A*
(2 2) *B* (*A*) :
(1 2) *B* : *E*(:)
(1 3) *B* : *E*(*E*(:) :)
(2 5) ( ) *B* : *E*(:)

6.3.11

H L 117 -

.

(1) : 1
(2) : 2
(3) : *E*(: 1 2)
(4) : *E*(: 1 2) *E*(: 1 2)
(5) : *E*(: 1 2) *E*(: 1 2)
(6) : *E*(: 1 2) *E*(: 1 2)
(7) : *E*(: 2)

T C , J R

37 . E ,

. T

:

(1 1)		:	1
(2 1)		:	1
(2 2)		:	2
(1 2)		:	2
(1 3)		:	$E($: 1 2)
(1 4)		:	$E($: 1 2) $E($: 1 2)
(1 5)		:	$E($: 1 2) $E($: 1 2)
(1 6)		:	$E($: 1 2) $E($: 1 2)
(1 7)		:	$E($: 2)
(2 3)		:	$E($: 1 2)
(2 4)	( )	:	$E($: 1 2) $E($: 1 2)
(2 5)	( )	:	$E($: 1 2) $E($: 1 2)
(2 6)		:	$E($: 1 2) $E($: 1 2)
(2 7)		:	$E($: 2)

(2.1). H 2 . T - . T

(1.5) (2.5) ( ) - . T 37 . T

.

L - 76 .

6.4

6.4.1 -

T 87 (*3*). P *A* *B* - . F ( ) *C* (- -). H (1). , *C* ( ) *A*. N . *A* *B* - . H

CS

.

(1) A : A $E($: C)
(2) A : $E($: A C)
(3) A B : $E($: A C)
(4) B : B $E($: A C)
(5) B : $E($: A C)

6.5

6.5.1 5

T . T
: C;
C ; A.

C . A
D C
C . T
C
10. I

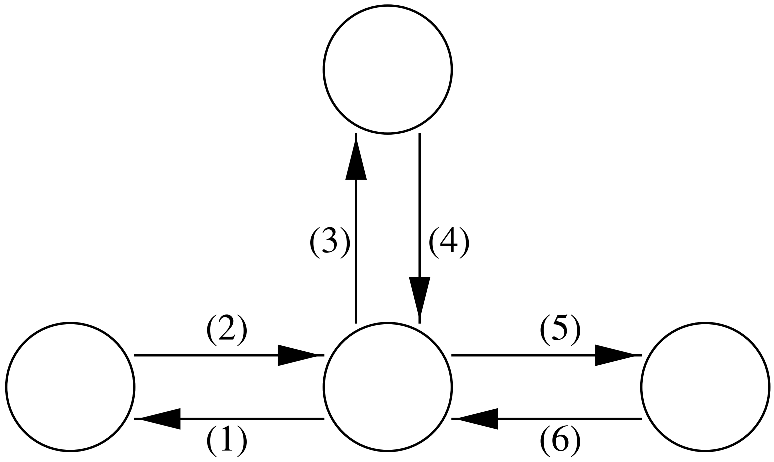
( ) . T ,
C .
A C . I
. A , C
.
T C A.

(1) C A : 1 1
(2) A C : $E($: 1)

$E($: C)

I (1) C A

. A 1 . A
(
) C. I



F 10: K E

, , G,
. T
. T
A . *C*
(2)
. T
:

(3) *C* : 2 2 *A*
(4) *C* : *E*(: 2)

A *E*(: *C*)

E(: *C*)

T *C*
. T *A*
(3).
I *C*
.

(5) *C* : *A*
(6) *C* : *E*(:)

A *E*(: *C*)

H *A* ,
(5). -

. I ,
(6) .

6.5.2

T :
.
. I N S
P 90 , .

(1) *A* *B* : *A*
(2) *B* : *B* *E*(: *A*)
(3) *A* : *E*(: *B*) *E*(: *A*)
(4) *A* *B* : *E*(: *A*) *E*(:)

T .

(1) *A* *B* : *E*(: *A*)
(2) *B* *A* : *E*(:)
(3) *A* *B* : *E*(:)

A .
P 60 . T -
.

(1) (*A*) *B* : *A*
(2) *B* ( ) : *B* *E*(: *A*)
(3)
(4) (*A*) *B* : *E*(: *A* ( )) *E*(:)

T :

(1) (*A*) *B* : *E*(: *A* ( ))
(2) *B* (*A*) : *E*(:)
(3) (*A*) *B* : *E*(:)

T :

(1) (*A*) *B* : *E*(: *A*)
(2) *B* (*A*) : *E*(:)
(1) (*A*) *B* : *E*(: *A*)
(2) *B* (*A*) : *E*(:)
(3) (*A*) *B* : *E*(:)

I
.

6.5.3

H KLS . T
. T *B*.

(1) *A* *B* : *A*
(2) *B* : *A* *B*
(3) *B* : *E*(: *A*) *E*(: *B*)
(4) *B* *A* : *E*(: *B*) *E*(: *A*) *E*(:)
(5) *A* *B* : *E*(:)

T :

(1) *A* *B* : *E*(: *A*)
(2) *B* *A* : *E*(:)
(3) *A* *B* : *E*(:)

T
N S -
.

6.5.4

I 1995, K C -
N S
67 .

(1) *A* : *A* *B*
(2) *B* : *E*(: *A* *B*) *E*(: *A* *B*)
(3) *B* *A* : *E*(: *A* *B*) *E*(:)
(4) *A* *B* : *E*(:)

T (D -
S N S). T -
( )
. T :

(1) *A* : *A B*
(2) *B* : *E*(: *A B*) *E*(: *A B*)
(3) *B* *A* : *E*(: *A B*) *E*(:)
(4) *A* *B* : *E*(:)

T .

(1) *A* : *A B*
(2) *B* : *E*(: *A B*) *E*(: *A B*)
(3) *B* *A* : *E*(: *A B*)
E(:) *E*(: *A B*)
(4) *A* *B* : *E*(:) *E*(: *A B*)

6.6

A ISO P 3 ISO/IEC
9798 S 63 .

6.6.1 -

(1) *A* *B* : *C* *B* 2 *E*(: *B* 1)

6.6.2 -

(1) *B* *A* : 1
(2) *A* *B* : *C* *B* 3 *E*(: *B* 2)

6.6.3 -

(1) *A* *B* : *C* *B* 2 *E*(: *B* 1)
(2) *B* *A* : *C* *A* 4 *E*(: *A* 3)

T
.

6.6.4 -

(1) *B* *A* : 1
(2) *A* *B* : *C* *B* 3 *E*(: *B* 2)
(3) *A* *B* : *C* *A* 5 *E*(: *A* 4)

T - (3) .

6.6.5

(1) *A* *B* : *C* 1
(1) *B* *A* : *C* 2
(2) *B* *A* : *A* 6 *E*(: *A* 5)
(2) *A* *B* : *B* 4 *E*(: *B* 3)

6.6.6

(1) *B* *A* : *B* *E*(: *B*)
(2) *A* *B* : *E*(: ( ) *A*)
(3) *B* *A* : *E*(: ( ))

6.6.7

I D -H
A *B*. L . T

(1) *A* *B* :
(2) *B* *A* :

A *B*
(1). *B*
A (2). *A* *B*
. T
. T
.

6.7

6.7.1 -

T 87 . I
G L .

(1) *A* : *A* *B*
(2) *A* : *E*(: *B*)
(3) *A* *B* : *E*(: *A*)
(4) *B* : *B* *A*
(5) *B* : *E*(: *A*)
(6) *B* *A* : *E*(:)
(7) *A* *B* : *E*(:)

L (74). M 1, 2, 4
5
:

(3) *A* : *E*(: *A*)
(3) (*A*) *B* : *E*(: *A*)
(6) *B* (*A*) : *E*(:)
(6) *A* : *E*(:)
(7) *A* : *E*(:)
(7) (*A*) *B* : *E*(:)

6.8 /

T *C*
A -
. I .

(1) *C* *A* : *C*
(2) *A* *C* : *A* *E*(: *A* *C*)
(3) *C* : *C* *E*(: *C* *E*(:))
(4) *A* : *C*
(5) *A* : *A* *E*(: *A*)
(6) *C* : *C* *E*(: 1)

T ( ) H
C 59 G L .

I :

(1) A :
(2) A : A E(: A)
(3) (C) : C E(: C E(:))
(4) (A) : C
(4) ( ) A :
(5) A : A E(: A)
(6) (C) : C E(: 1)

I :

(1) C (A) : C
(1) (C) A : C
(2) A C : A E(: A C)
(3) C ( ) : C E(: C E(:))
(4) A : C
(5) A : A E(: A)
(6) ( ) C : C E(: 1)

I (G L) (3)
- .

6.8.1 /

H C 59
( ) SPLICE . T
SPLICE/AS C J -
.

(1) C A : C
(2) A C : A E(: A C)
(3) C : C E(: C E(:))
(4) A : C
(5) A : A E(: A C)
(6) C : C E(: 1)

F (3)
(6)
.

(3) C ( ) : C E(: C E(:))
(3) : E(: E(:))
(6) : E(: 1)
(6) ( ) C : C E(: 1)

T
(3). I C (3) (3)
.

6.9

T -
A *B* .
A *B*.

(1) *A* : *A* *B*
(2) *A* : *C* *C*
(3) *A* *B* : *C* *C* *E*(: *E*(:))

C *E*(: *A*) *A*
. T (A 1994).
B *A*

(3) *B*(*A*) *C* : *C* *C* *E*(: *E*(:))

A *C*.

6.9.1 .509

T , 26 , (-
1, 1 2 . I
.

(1) *A* *B* : *A* *E*(: *B* *E*(:))
(2) *B* *A* : *B* *E*(: *A* *E*(:))
(3) *A* *B* : *A* *E*(:)

A LA M 12 B -
A N 26 . T -
. I

.

6.10

6.10.1

T . I
.
I . I
.

(1) *A* *B* : *E*(:)
(2) *B* *A* : *E*(: *E*(:))
(3) *A* *B* : *E*(:)

T *A* .

(1) *A* (*B*) : *E*(:)
(2) (*B*) *A* : *E*(:)
(3) *A* (*B*) :

C
(2) ,
, *C*
B .
T :

(1) *A* (*B*) : *E*(:)
(1) (*B*) *A* : *E*(:)
(2) *A* (*B*) :
(2) (*B*) *A* :
(3) *A* (*B*) : *E*(:)

6.10.2

T 50 -
. I - (
) ( ). E *A* *B*
, , . ,
.

(1) *A* *B* : *A* *B*
(2) *B* : *A* *B*
(3) *B* : (*A*) ( ) ( )
(4) *B* *A* :
(5) *A* *B* :

I (3) ( ) (*B*) .
A *B*, -
. T OR . P *B*
(*A*) ( )
. I ( )
. A (4). *A* -
(*B*) ( ) . I
B *A* (5). T
.

6.10.3

T B M 15
:

(1) *A* *B* : *E*(:)
(2) *B* *A* : *E*(: *E*(:))
(3) *A* *B* : *E*(:)
(4) *B* *A* : *E*(:)
(5) *A* *B* : *E*(:)

H ,
. . T

( )

(1 1) *A* (*B*) : *E*(:)
(2 1) (*B*) *A* : *E*(:)
(2 2) *A* (*B*) : *E*(: *E*(:))
(1 2) (*B*) *A* : *E*(: *E*(:))
(1 3) *A* (*B*) : *E*(:)
(2 3) (*B*) *A* : *E*(:)
(2 4) *A* (*B*) : *E*(:)
(1 4) (*B*) *A* : *E*(:)
(1 5) *A* *B* : *E*(:)
(2 5) (*B*) *A* : *E*(:)

6.10.4

T D S 40
. T :

(1) *B* *A* : *E*(: *A*)
(2) *A* : *E*(: *A*) *B*
(3) *A* : *E*(: *B*)

O (3) *A* *B*
A. I *B* *C* *C*
(3) *E*(*C* *B* :). *B*
A (1). S
(C J). T
.

A .

(1) *B* *A* : *E*(: *A*)
(2) *A* : *E*(: *A*) *E*(: *B*) *E*(: *A*)
(3) *A* : *E*(: *B*)

H .
. *E*(: *A*) *A*
.

T :

(1) *B* : *E*(: *B*)
(2) *B* : *E*(: *B*) *E*(:)

A :

(1) *A* : *E*(: *A*) *B*
(2) *A* : *E*(: *A*)*E*(: *B*)
(3) *A* *B* : *E*(: *A*) *E*(: *A*)

T S R P
P R D E R A . T
. I -
, P R , I , G L
C R . J C L
C S J J L C S
U .

1 M A R N . P E P
C P . T , SRC DIGITAL, J
1994.

,
. R , .

.
, .
I ,
, .
.

.

E ;
.

.

( ) . P 2
, .
:

I
, -
.
(D A -
K E L
).
B . E

. E
.

K -
.

-

. O , -

.

F

CCI .509 .

B .

-

, .

, -

. B -

.

I

. F

.

A ,

, , . R

.

I ,

. I

,

,

,

.

2 J. A . C = P ? *EEE* , 29 35,
A 1992.

A

D . N A -

D (R A)

R R . A .

3 S G. A . D S : A T S . *C* ,
15 24, F 1983.

(1983). P ,

. B

. A .

4 R A . UEPS A S G E . I
. D , G. E , J.-J. Q , ,
E C 92 . S LNCS 648, 1992.

I , -
E P
(EP). . A
BAN EP .

5 R A . C F . *C AC* ,
N 1994.

A M -
. -
A M .
.
A M ;
. H ,
. M
. F ,
. A -
C EC I EC
- .

6 R A . M S S R . I *C 94* ,
1994.

-
. A
(
). E P (EP) -
.

7 R A . L C S : N P .
I D G , , *E C 94* , 231 245.
S LNCS 875, 1994.

.
- -
, A
K. N -
.

8 R A . C E M , P -
L . A RA P
:// . . . . / / 14/.

E . I
. A -
. - -
(A M
).
(-
).
G .
,
, -
.

9 R A J B . O R
E P S . A RA P
:// . . . . / / 14/, 1995.

I - -
A . -
.

10 R A R N . P S -
C . A RA P
:// . . . . / / 14/, 1995.

.
. - -
(L
116 , L N 74 ,
A D , -
M F (
) .

A -
. R .
A : -
. A .

11 R A R N . R P
P K P . A RA P
:// . . . . / / 14/, 1995.

. -
. P -
E (

).

12 C A C M . S D CCITT
R .509 T D A F -
. *C* *C* , 20(2):30 34, A 1990.

CCI 509 -
. :

8.1
R A (
);

(
)
( );

-
(
);
R A (
)
.

A . F ,
(, C J
34 PLICE/A , -
59 , .

13 M B , J K , P R . T S C -
B C . I G. D , , *A* *C* -
- *C* *94* , 839 LNCS, 341 358. S
, 1994.

CBC
. O . A .
106 .

14 S. M. B M. M . L K A -
S . *C* *C* , 20(5):119 132, O -
1990.

I -
K .
, , ,
, .
.
. A .

15 S. M. B M. M . E K E : P
. I *1992*
EEE , 72 84.
IEEE C S , M 1992.

(EKE). I -
( )
. A
. A
. -
. I .
(. .
.).
R A E G .

16 P. B . A L C H E . I
C ,
14 22. IEEE C S P , 1990.

K 5
(
). E -
.

17 P B N B -C . F
. 1993.

B -
. A
. B .

18 R. B , I. G , A. H , P. A. J , S. K , R. M ,
M. . S D T -P A P -
. I J. F , , *C* *91: A*

C , 576 L N C S ,
44 61. S , 1991.

. I -

. .

19 R. B , I. G , A. H , P. A. J , S. K , R. M ,
M. . S D F A -R A -
. *EEE* *A* *C* ,
11(5):679 693, 1993.

-
3-
. -
. I -
.

20 A. D. B . S C R P C .
AC , 3(1):1 14, F 1985.

A RPC P . A
26 .

21 C B . H A C P . -
EE , 137 P E(6):433 436, N 1990.

A , .

.
(N - 88 O -R 91)
. -
C B C (CBC) DE ( )
( ) . A -
(
).

.
-

.
P CBC
. - ,

( )

.

22 C B . A C F E K M P -
. I *9 EEE C* -
, 2 8. IEEE C S P , 1996.

-
. A
.
.
. K B
.
.

23 C B M . O L BAN L . I T
H , , *E 93* , 765 LNCS, 240 247.
S , 1993.

B M BAN -
. .
( ) -
. - -
; .

O 120 .

24 C B M . D S K E P -
. I D G , , *C E C 94* ,
93 106. S - , 1994.

, . .
. I
. A
.
. I ,
( )
.

( ), , .
( )
.

(-
,).

(,

).

. -

.

. I -

(

, . .) . F -

, (1)

. I

. A

- .

25 E. F. B A. M. O . C : A S R
R . *EEE* , 76(5), M 1988.

(1988) -
. A
, O - - O - -
, R A . I D E -
.

26 M B , M A , R N . A L
A . T R 39, D S R C -
, F 1989.

.

.

1 A

, .

. I

. A

.

(

).

:

, ,
,
.

BAN .
-

I J
J -
J
, .
I J

J .
I J ,
J .
I J

J .

2 I
- . M .
, . A
.

. (,
). M ,
.

. -
. I ,
. -
. I , ,
: :
.

:
;

.

. . F

, ,

;

.

. M .

I (I

, I , -

) -

-

.

.

. -

. -

.

P ;

BAN . E

.

.

-

. O , . .

.

L , -

. .

. F

.

I

, ,

.

1. .
2. A .
3. L , -
.

4. -

,.

E

.

( ) ,

.

3

.

, .

4 11 BAN

:

O -R P

N P .

K P

- F P

A RPC H

P

N - P K P

CCI .509 P ( )

.

12 13 -

.

. M ,

, (

).

.

27 M B , M A , R M. N . R N . *AC* , 24(2):39 40, A 1990.

BAN N 89 .

26

. .

N

.

. F ,N
.

! P BAN .

28 M B , M A , R M. N . T S
L A . R R R 39, D
S R C , 1994.

BAN 26 .

29 C. C. I. T. T. R .509. *D -A*
. C. C. I. T. T., D 1988.

.

30 E. A. C , R. S -N , P. A. P . P B
P R A S P . I
5 EEE C ,
84 91. IEEE C S P , 1992.

A ; (-
) .

.
. L -
.

. .

.

31 U C . C P F . I *7 EEE*
C , 192 200. IEEE C -
S , 1994.

. :

. . , N
89 BAN .
(,

)

. D -
42 N -
. B A N
A RPC 26 .

. - -
(. .
). - R , A -
. -
:

(1) : (:)
(2) : (: (:))
(3) : (:)

A 2 -
3.
-
2 3. -
(
) . A
,

.
.
-
,
( ) -
. F -
:
;
;
;
( ) ;
.
N -
O -R .
-
(. .).
- -

.

-
.
- . O -
.

32 U C . G F C P S -
. I *7 EEE C* -
. IEEE C S P , 1994.

-
. . I
-
. R -
(, ,),
. I (-
,
. A , . A
CK 5 . P
,
. O (
) . A
- .

33 U C . O P A P
C S . , 28(3):16 23,
1994.

-
(PC). .
(. .) -
. .
( ). O -
(5
RCE).

34 J C J J . O T S R P .
, 56(3):151 155, N 1995.

I -
( ) PLICE (
L P R G
O).

35 J C J J . A .
, 1(5):465 474, A 1996.

-

. M :

, , , -

(. . B -

). A

!

36 J C J J . N -R N E .

A .

. I -

.

37 J C J J . F N E : N
T N G M P .

I -

L 117 6.3.11.

M

.

38 D. C . T D E S (DES)
. *B* *D* ,
38(3):243 250, M 1994.

I DE -

.

IBM 1974.

!

G .

- .

A .

39 D. . D . L. P . *C* . J
S , 1 , 1994.

-

. I -

.

.

40 D D R S . N S P -K C .
, 64 67, 1990.

A -
. , . -

. (
). O -
:
-
(
).

.

41 D. E. D . *C* *D* . A ,
1982.

. I -

- .

42 D D G. S . T K D
P . *C* *AC* , 24(8), A 1981.

N -
87 . -
. B
(
,
, -).

H ,
. .

. F
.

1994 M A (6.9).

A - . A .

43 D . T F T P K C .
EEE , 76(5):560 577, M 1988.

A . -
(-
, , R A, -).

. A .

44 . D M. H . N D C . *EEE*
, 22(6):644 654, N 1976.

A . H .

45 *46* *D* *E* -
, 1976.

D E . I -
. .

46 . F P. L . P K M . *EEE*
A *C* , 785 793, J 1993.

. I

. I .

47 P G , D J , J H , B R . S -
M CSP FDR: D B 2. T
, F S (E) L , A 1996.

C P/FDR . -

(-
.). I ( ) . -

C P (FDR2) . L
-
. I
(. . CBC, CFB) ;
.

48 P G , D J , B R . S M
CSP FDR: D B 3. T , F
S (E) L , J 1996.

47 . -
CCI . O -

(
).

49 D G . E A ? I
1996 EEE ,
46 54. IEEE C S , 1996.
. I
G 4 . H
-
. E . H
-
.
- -
.
.

50 L G . U O - F A . *C*
C , 19(5):8 11, O 1989.
( ) - . -
. -
. I -
-
.

51 L G . A N R E M . *C*
C , 20(5):18 22, O 1990.
R
. E
. A -
. A
. P , ,
. I -
( ) -
. E .

52 L G . H I S C P -
. I *4 EEE C*
, 99 102. IEEE C S , J 1991.
BAN 26 .
GN 55

.
. ,
. I
.

53 L G . T M F R-
R , D D F N
A C P . I *6 C* -
, 131 136. IEEE C S
P , 1993.

. :
;
;
, -
.
, , -
, ,
.
. A
.

54 L G , A. L , R. N , J. S . P P
C S G A . *EEE* *A*
C , 11(5), 1993.

I ,
. A
. F -
.
. -
.
.
.

55 L G , R N , R . R A
B C P . I D C T
L , , *1990 EEE* -
, 234 248. IEEE C S , M 1990.

BAN 2 6 . I
(
), (-
, ,).
I BAN- -
( ). A
- -
. -
.
(40) BAN.

56 J G . P K C . I
84, 1984.

.
-
.
- , , ,
.
I (-
)
(. . -
). M -H R A
.

57 R. H , P. J , R. M , G. T , E. H .
R S P K C M . I D
G , , *C* *E* *C* *94* , 875
L N C S , 107 122. S , 1994.

(,
).
K (4 5) CHANGEP
(4).
-
.
A . I -
(
)
. E ( )
( ) (

).

-

. D

. I

, -

. (

) -

( )

( ).

I . I

.

. .

58 M E H . T M P K C .
A , 130 139, A 1979.

-

. NP-

R A .

.

A .

59 T H -H C . O
SPLICE/AS: T IDE I . -
, 53:97 101, 1995.

PLICE/A -

. .

. C J 34 .

60 T H , N - L , C -M L , M - K ,
-H C . T A N -S A -
P . , 53:103 107,
1995.

N .

C 31 1994 (-

C).

.

.

(-

). I

.

I ,

;
.

. E
. ,
.

61 ISO/IEC. - *E* *A* -
1: , 1991.

I O/IEC 9798 -
. I
.

62 ISO/IEC. - *E* *A* -
2: E
, 1993.

I O/IEC 9798 -
. A
-
(. . ,).

63 ISO/IEC. - *E* *A* -
3: E
, 1995.

I O/IEC 9798
.
.

64 ISO/IEC. - *E* *A* -
4: E -
, 1993.

I O/IEC 9798 -
.

65 ISO/IEC. - *E* *A* -
5: E -
, 1993.

I O/IEC 9798 -
. A
(. . ,).

66 A J , J S , . B B A . I
D G , , *C* *E* *C* *94* ,
875 L N C S , 125 142. S ,
1994.

B - .
C R (
) . A -
1 .

. (H -
/ ?)

,
( ) 1 2. L (1
2) .
. A . I , 1
(1
/
).

A N .

.

67 I L K R C . A E S A -
P U U K . ,
29(3):14 21, J 1995.

. -
, . .
.

68 A. K , J. S , H. L . A N -B
P M A . ,
26(4):84 89, 1992.

A . A

. R
(
) .
A BAN 26
.
( ).

,
109 . I -
. I N 90 -
.

, -

. I BAN
.

F
.

69 R. A. K . U F T A
E P . I *1987 EEE*
, 134 139. IEEE C S -
P , 1987.

( ). I
J (-
).
- -
.

70 C. M R. K J M . T S
C P A . *C* , 7(2):79 130,
1994.

A . : I , NRL
P A I J .
MN . .

71 . K G. . AUTLOG A -
. I *C*
, 90 99, 1994.

BAN L 26 . I -
(. .)
. I -
B A N .

.
. .
(N

89).

.

72 P C. K . C D -H , RSA, DSS,
S U T A . E A PK
P :// . . . . / / 14/, 1995.

A

.

.

.

E !.

73 A L . A D S : A B -
. , 27(4):122 136, O 1993.

-
. I -
, ,
(, , , - .) -
.

.

!

74 G L . A A N -S P K A -
P . , 56(3):131 136,
N 1995.

N P K
87 L
. .
FDR .

75 G L . B -
. I *ACA* , 1055,
147 166. S , 1996.

I L C P FD R
N
P K P 6.7.1. H -
C P (
)

.

76 G L . S N A S P . I -
C . IEEE C -
S P , 1996.

.

. L
M A P C J (
) (6.3.11).
. L

. L
. A
K L 6.5.3 MN .

77 G L . SPLICE-AS: A C S U CSP D E -
S P . T , P R
G , O , 1996.

I C P FDR
(-
).

78 M C B . T F A S -
P . I *C*
, 147 158. IEEE C S P , 1993.

I BAN . A -
BAN
. F -
(-),
(-
).
. -
. A -

(. . ,
.). A BAN- .
.

79 M C B . D A P -
: S M N A . I *7*
C , 178 186. IEEE C -
S P , 1994.

-
. -
. B
M
-
. ,
.
-
.

O -R .
,
.

-
.
.
O , - , .

80 M C B . O S A P -
F C . I D G , , *C*
E *C* *94* , 875 L N C
S , 193 204. S , N 1994.

- . A K -
.

.
: ,
, , , , , -
, . N
. F .
. I
( ) . H ,
.
M
. N -
? B
,

. CBC
. ,
.
A K K .
. R -
. I
MAC . -
. A
.

81 J L. M . A I C C .
EEE , 76(5):533 549, M 1988.

A , -
. .
.

.

82 C M . F : A
. I *A* *96* , 1996.

M -
. A
. F ,
(. . -
) .

83 J M . T I U G . T R M
93B0000172, MITRE, 202 B R , B , MA 01730-1420,
1994.

I -
. -

. I -
(N -
, D H E MN).

.
A .

84 J. K. M , S. C. C , S. B. F . T I : P -
S A . *EEE* *E* ,
13(2):274 288, F 1987.

I . 83
.

85 J H. M . P F C .
EEE , 76(5), M 1988.

.
,

. I -
.
R A :

; -
; -
(
). F .
-
. A
.

. -
( ).

86 L E. M . A L K B C
S . I J T H , , *C* -
, 57 63. IEEE, C S
P IEEE, 1989.

-
. I -
-
- . F
( ) ( ) ( ) -
. A . P
. A
18 .
-
, ,
.
. -
, -
(A 1
).

A . -
.
F . C
. C
( ).
-
. B
. A , .

87 R N M S . U E A -
L N C . C
AC , 21(12), D 1978.
O . I -
,
- (,)
.
:
. 42 . I
N P
. -
. -
G L .
.
. A ,
.
- :
,
.
,
.
O . E .

88 R M. N M. D. S . A R .
, 21(7):7 7, J 1987.

I ( )

D (
) 42 .
. -

, .

89 D M. N . A C B , A N
L . *AC* , 24(2):35 38, A 1990.

( ) -
BAN B , A N -
BAN ( ) 26 ,
( ) BAN
(,).

N ( ) BAN -
. BAN
.
; BAN -
. I ,
BAN O R
, -
N (
107).

-
BAN -
.

-
. ( )
.
.

.

90 B. C N S G. S . A N U
T N . , 27(2):10 14, A
1993.

K
68 .
. I , ,
, -
.

BAN 26 KL
68 , . F
.
(. .) .
H 60 .

91 D. O O. R . E T M A .
, 21(1):8 10, J 1987.

- O -R .
. -
:
(. . BAN 26). -
.

92 R. R , A. S , L. A . A M O D -
S P K C . *C*
AC , 21(2):120 126, F 1978.

R A
(M G).
A .

93 A. . R . I S S P . I
9 EEE C ,
28 38. IEEE C S P , 1996.

: -
.

A (
). G
-

.
. A
. I
. A -
. O
(. . BAN).
C C P FDR
. .
R P
DERA.

94 B R P G . S M CSP FDR:
F R . T , F S E , 1995.

C P -
. A
FDR

. -
F C P/FDR
.
R P DERA.

95 A. D. R P. H . F M A
A P . T R T 93 7,
CITI, N 1993.

-
.
N - 87 ,
.
. -
. - .

96 P R . T D S P . T -
, D E R A , A 1996.

-
C P FDR
. ,
C P .
(,
, ,). E
.
-
.

97 S S . S P CSP. I
1996 EEE , 174 187. IEEE
C S P , 1996.

-
C P .
C P
.

98 B. S . T IDEA E A . *D . D* ,
50 56, D 1993.

, IDEA
. 64-
128- .
.

1.5 2 -
DE . L I
177MB / 35MH .

99 B S . *A C* . , 1994.

P -
. I
. M -
. A
. -

.

100 G.J. S . H I D A T
C T . *EEE* , 76(5):621 627,
M 1988.

A ! R ,
( ) -
L . D
.

101 M E. S D K. B . T D E S -
: P F . *EEE* , 76(5):550 559, M
1988.

. I DE ,
,
. A . N -
198 8.

102 E S . E BAN A P A -
. I *1991 EEE* ,
171 181. IEEE C S P , 1991.

BAN
. H BAN
-

. A
D N 89 .

103 E. S . R C P . I
1992 EE . IEEE C S
P , 1992.

I B -
16
. B , ,
. A BAN
B CK 5 .

104 E S . *A C*
. P D , F M N S ,
U O , N D R E ,
P.O. B 25, N-2007, K , N , 1995.

DP -
. N HOL -
.

105 J G. S , C N , J I. S . K -
:A A S O N S .
1988.

K .
.
.

106 S G. S D. G . O M I
C P . I *1992 EEE*
, 85 104. IEEE, 1992.

. -
(CBC). K -
. -
( )
. A .

107 P S . T U L A C
P . I T F. L J M L , ,
1991 EEE , 156 170.
IEEE C S , M 1991.

-
. I

. H
.

2 :
( )
( ). L , , -
, -
.

, -
. P

.

3: BAN
26 BAN.
BAN
,
. I
. N 89 . -
BAN
, .
O BAN
, -
. . . ,
. H

-
.
C G .
H N
BAN ( )
. H BA N
BAN
.
I BAN
. A , ,
BAN .

4: . O
-
. G , . A -
,
. A

.
, -
(
). A
( ).

N .

O : .

108 P S . A T O R A . I
7 EEE C , 131 136.
IEEE C S P , 1994.

; , -
: (
) (
). O
- (-
) - (-
). R - -
( ) (
).

:
(
) (
).

(, BAN
).
BAN- .
-
. I
.
.
. .

-
?

109 P S . O K D R A .
I , 24 30, 1994.

- N
.
(,
). A
N -
, ,
. A
K L 68 .
K L N -
BAN 26
.

A , .

110 P S C M . A L S -
C P R . I
1993 EEE , 165
177. IEEE C S P , M 1993.

A . H .

111 G T . M A O - H F -
. , 22(5):29 38, 1992.

: -
. .

112 L. S T. K . S M
H -L N P . *C* , 15(2):135 171,
J 1983.

A . -
. B
(, -

DE). E .

113 *E DE* , C 93, A 1993.

-
DE . A . P
!

114 M . C O N . C ,
1:177 186, 1982.

-
. I
. I -
. I C DE
( ).

115 M . A T P K C . C
, 1 20, 1982.

-
(R A M H K).

116 T. . C. S. S. L . A D S .
C , 25(1):39 52, J 1992.

-
, , ,
.
.
(K P) . .
L -
5 47 :
5 6.
. I ,
L -
117 .

117 T. . C. S. S. L . A L A P
D . , 24 37, 1994.

A 116 -
.
( ) -
.
-
. ,
.
A .

. I

.

.

E

-

-

.

118 S. , K. O , H. M . D I -
A S IDE I E -
. I *10* *C* *C*
C , 1990.

PLICE A . 34 .

119 A F A . A F S E -
C P . T
IEEE S S
P 1994., 1993.

-

. I

. A ( )

.

:

O

. A

.

,

. . ,

.

A CPAL (C P A L)

. BAN

,

. CPAL -

(/ ,

, , , / -

) . N

( ).

-

-

(. .).

CPAL

(N

P K P , D P K P ,

O R P K P).

.

120 P C O . A A E BAN L
. I T H , , *E* *93* , 765
LNCS, 443 447. S , 1993.

B M -

BAN 23 . O -

( ) BAN

. BAN -

.