Capítulo 14

Tabela 14.1 Resumo das trocas de mensagem do Kerberos versão 4

(1) C → AS $ID_c \| ID_{tgs} \| TS_1$

(2) AS → C $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| TempodeVida_2 \| Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| TempodeVida_2])$

(a) Troca de serviço de autenticação para obter ticket de concessão de ticket

(3) C → TGS $ID_v \| Ticket_{tgs} \| Autenticador_c$

(4) TGS → C $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| TempodeVida_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| TempodeVida_4])$

$Autenticador_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

(b) Troca do serviço de concessão de ticket para obter ticket de concessão de serviço

(5) C → V $Ticket_v \| Autenticador_c$

(6) V → C $E(K_{c,v}, [TS_5 + 1])$ (para autenticação mútua)

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| TempodeVida_4])$

$Autenticador_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

(c) Troca de autenticação cliente/servidor para obter serviço

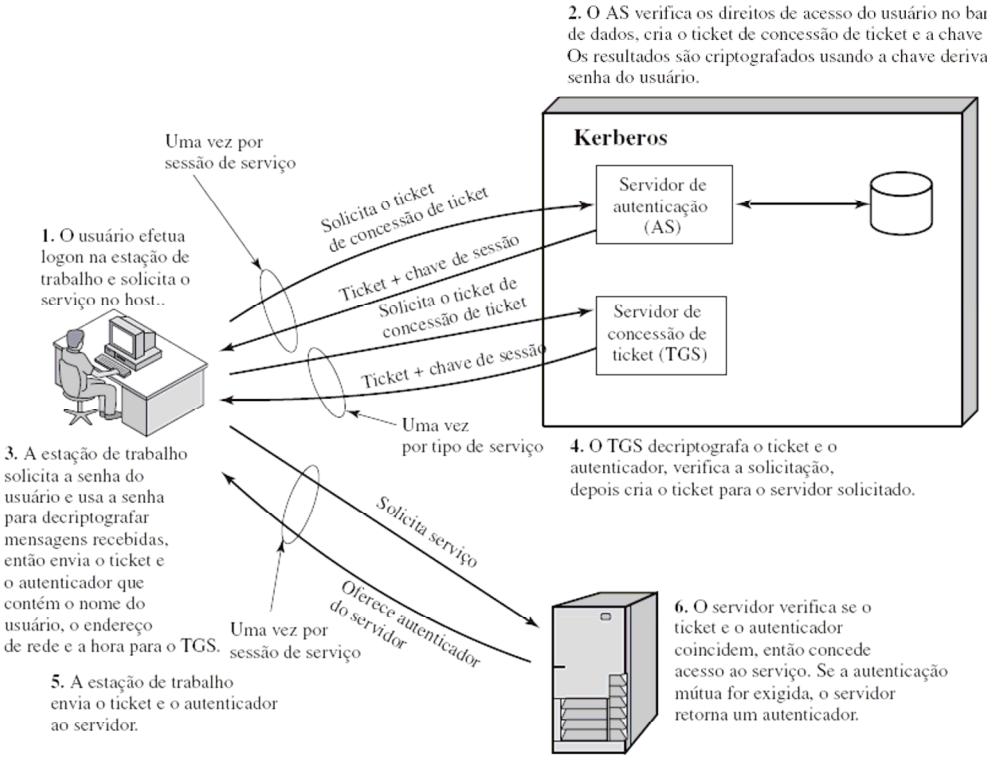

Figura 14.1 Visão geral do Kerberos.

Tabela 14.2 Razões para os elementos do protocolo Kerberos versão 4

Mensagem (1)	O cliente solicita o ticket de concessão de ticket
ID_C	Diz ao AS a identidade do usuário a partir desse cliente
ID_{tgs}	Diz ao AS que o usuário solicita acesso ao TGS
TS_1	Permite que o AS verifique se o clock deste cliente está sincronizado com o do AS
Mensagem (2)	O AS retorna o ticket de concessão de ticket
K_c	A criptografia é baseada na senha do usuário, permitindo que o AS e o cliente verifiquem a senha, e protegendo o conteúdo da mensagem (2)
$K_{c,tgs}$	Cópia da chave de sessão acessível ao cliente, criada pelo AS para permitir a troca segura entre cliente e TGS sem exigir que compartilhem uma chave permanente
ID_{tgs}	Confirma que esse ticket é para o TGS
TS_2	Informa ao cliente sobre a hora em que esse ticket foi emitido
$TempodeVida_2$	Informa ao cliente sobre o tempo de vida desse ticket
$Ticket_{tgs}$	Ticket a ser usado pelo cliente para acessar o TGS

(a) Troca do serviço de autenticação

Mensagem (3)	O cliente solicita o ticket de concessão de serviço
ID_V	Diz ao TGS que o usuário solicita acesso ao servidor V
$Ticket_{tgs}$	Garante ao TGS que esse usuário foi autenticado pelo AS
$Autenticador_c$	Gerado pelo cliente para validar o ticket
Mensagem (4)	O TGS retorna o ticket de concessão de serviço
$K_{c,tgs}$	Chave compartilhada apenas por C e TGS protege conteúdo da mensagem (4)
$K_{c,y}$	Cópia da chave de sessão acessível ao cliente, criada pelo TGS para permitir a troca segura entre cliente e servidor, sem exigir que compartilhem uma chave permanente
ID_V	Confirma que esse ticket é para o servidor V
TS_4	Informa ao cliente sobre a hora em que esse ticket foi emitido
$Ticket_V$	O ticket a ser usado pelo cliente para acessar o servidor V
$Ticket_{tgs}$	Reutilizável de modo que o usuário não precise reinserir a senha
K_{tgs}	O ticket é criptografado com a chave conhecida apenas pelo AS e pelo TGS, para impedir modificações
$K_{c,tgs}$	Cópia da chave de sessão acessível ao TGS, usada para decriptografar o autenticador, autenticando assim o ticket
ID_C	Indica o proprietário que tem direito a esse ticket
AD_C	Impede o uso do ticket a partir de uma estação de trabalho que não seja aquela que solicitou o ticket inicialmente
ID_{tgs}	Garante ao servidor que ele decriptografou o ticket corretamente
TS_2	Informa ao TGS sobre a hora em que esse ticket foi emitido
$TempodeVida_2$	Impede a repetição depois da expiração do ticket
$Autenticador_c$	Garante ao TGS que o apresentador do ticket é o mesmo cliente a quem o ticket foi emitido; tem muito pouco tempo de vida, para impedir repetição
$K_{c,tgs}$	O autenticador é criptografado com a chave conhecida apenas pelo cliente e pelo TGS, para impedir modificação
ID_C	Precisa coincidir com o ID no ticket para autenticar o ticket
AD_C	Precisa coincidir com o endereço no ticket para autenticar o ticket
TS_3	Informa ao TGS sobre a hora em que esse autenticador foi gerado

(b) Troca de serviço de concessão de ticket

Mensagem (5)	O cliente solicita o serviço
$Ticket_V$	Garante ao servidor que esse usuário foi autenticado pelo AS
$Autenticador_c$	Gerado pelo cliente para validar o ticket
Mensagem (6)	Autenticação opcional do servidor ao cliente
$K_{c,v}$	Garante a C que a mensagem é de V
$TS_5 + 1$	Garante a C que essa não é uma repetição de uma resposta antiga
$Ticket_v$	Reutilizável de modo que o cliente não precisa solicitar um novo ticket do TGS para cada acesso ao mesmo servidor
K_v	O ticket é criptografado com chave conhecida apenas pelo TGS e pelo servidor, para impedir modificações
$K_{c,v}$	Cópia da chave de sessão acessível ao cliente; usada para decriptografar o autenticador, autenticando assim o ticket
ID_C	Indica o proprietário que tem direito a esse ticket
AD_C	Impede o uso do ticket a partir de uma estação de trabalho que não seja aquela que solicitou o ticket inicialmente
ID_V	Garante ao servidor que ele decriptografou o ticket corretamente
TS_4	Informa ao servidor sobre a hora em que o ticket foi emitido
$TempodeVida$	Impede a repetição depois da expiração do ticket
$Autenticador_c$	Garante ao servidor que o apresentador do ticket é o mesmo cliente a quem o ticket foi emitido; tem curto tempo de vida, para impedir repetição
$K_{c,v}$	O autenticador é criptografado com chave conhecida apenas pelo cliente e pelo servidor, para impedir modificações
ID_C	Precisa coincidir com ID no ticket para autenticar o ticket
AD_C	Precisa coincidir com o endereço no ticket para autenticar o ticket
TS_5	Informa ao servidor sobre a hora em que o autenticador foi gerado

(c) Troca de autenticação cliente/servidor

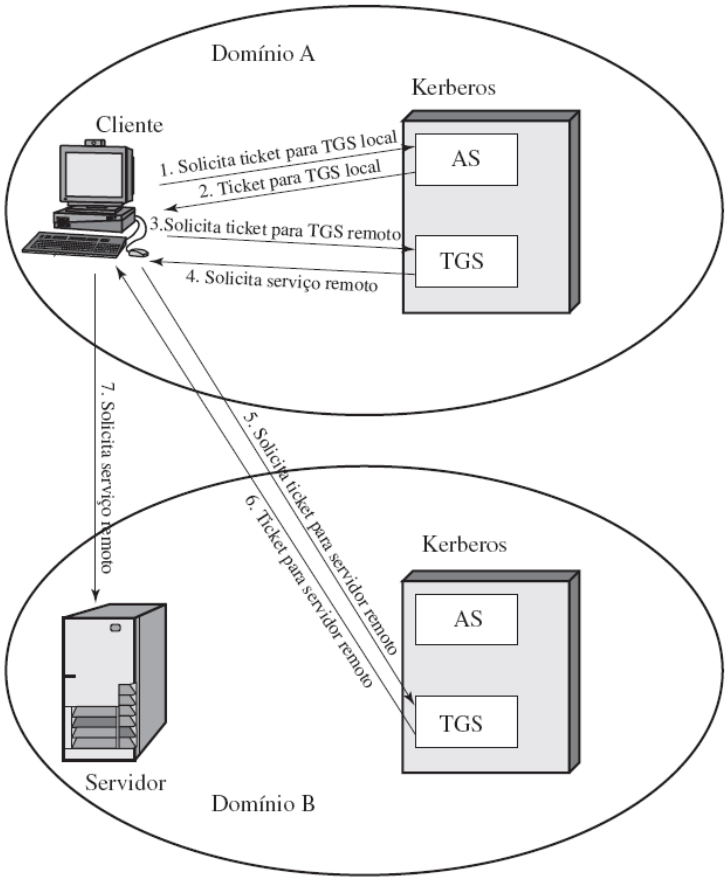

Figura 14.2 Solicitação de serviço em outro domínio.

Tabela 14.3 Resumo das trocas de mensagem do Kerberos versão 5

(1) C → AS $\text{Options} \| ID_c \| Realm_c \| ID_{tgs} \| Times \| Nonce_1$

(2) AS → C $Realm_c \| ID_C \| Ticket_{tgs} \| \text{E}(K_c, [K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}])$

$$Ticket_{tgs} = \text{E}(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$$

(a) Troca de serviço de autenticação para obter o ticket de concessão de ticket

(3) C → TGS $\text{Options} \| ID_v \| Times \| \| Nonce_2 \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $Realm_c \| ID_C \| Ticket_v \| \text{E}(K_{c,tgs}, [K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v])$

$$Ticket_{tgs} = \text{E}(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$$

$$\text{Ticket}_v = \text{E}(\text{K}_v, [\text{Flags} \| \text{K}_{c,v} \| \text{Realm}_c \| \text{ID}_C \| \text{AD}_C \| \text{Times}])$$

$$Authenticator_c = \text{E}(K_{c,tgs}, [ID_C \| Realm_c \| TS_1])$$

(b) Troca do serviço de concessão de ticket para obter o ticket de concessão de serviço

(5) C → V $\text{Options} \| \text{Ticket}_v \| \text{Authenticator}_c$

(6) V → C $\text{E}_{\text{K}_{c,v}}[\text{TS}_2 \| \text{Subkey} \| \text{Seq\#}]$

$$\text{Ticket}_v = \text{E}(\text{K}_v, [\text{Flags} \| \text{K}_{c,v} \| \text{Realm}_c \| \text{ID}_C \| \text{AD}_C \| \text{Times}])$$

$$Authenticator_c = \text{E}(K_{c,v}, [ID_C \| Realm_c \| TS_2 \| Subkey \| Seq\#])$$

(c) Troca de autenticação cliente/servidor para obter o serviço

Tabela 14.4 Flags Kerberos versão 5

INITIAL	Este ticket foi emitido usando o protocolo AS e não emitido com base em um ticket de concessão de ticket.
PRE-AUTHENT	Durante a autenticação inicial, o cliente foi autenticado pelo KDC antes que um ticket fosse emitido.
HW-AUTHENT	O protocolo empregado para autenticação inicial exigia o uso de hardware que deveria ser de posse apenas do cliente indicado.
RENEWABLE	Diz ao TGS que este ticket pode ser usado para obter um ticket substituto que expira em uma data posterior.
MAY-POSTDATE	Diz ao TGS que um ticket pós-datado pode ser emitido com base nesse ticket de concessão de ticket.
POSTDATED	Indica que este ticket foi pós-datado; o servidor final pode verificar o campo authtime para verificar quando ocorreu a autenticação original.
INVALID	O ticket é inválido e precisa ser validado pelo KDC antes do uso.
PROXIABLE	Diz ao TGS que um novo ticket de concessão de serviço, com um endereço de rede diferente, pode ser emitido com base no ticket apresentado. PROXY indica que este ticket é um proxy.
FORWARDABLE	Diz ao TGS que um novo ticket de concessão de ticket, com um endereço de rede diferente, pode ser emitido com base no ticket de concessão de ticket.
FORWARDED	Indica que o ticket foi encaminhado ou emitido com base na autenticação envolvendo um ticket de concessão de ticket encaminhado.

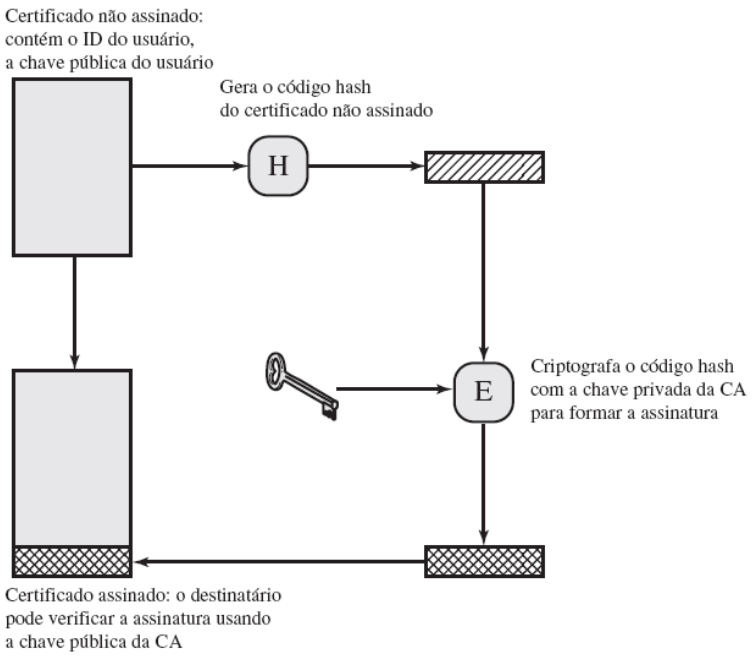

Figura 14.3 Uso do certificado de chave pública.

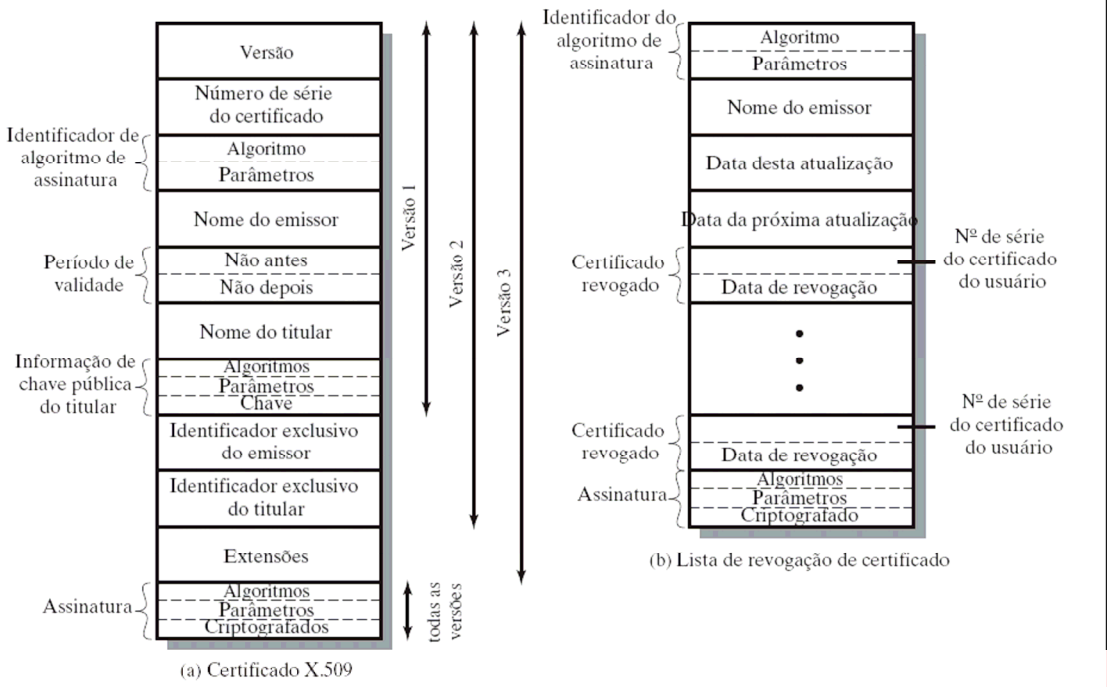

Figura 14.4 Formatos X.509.

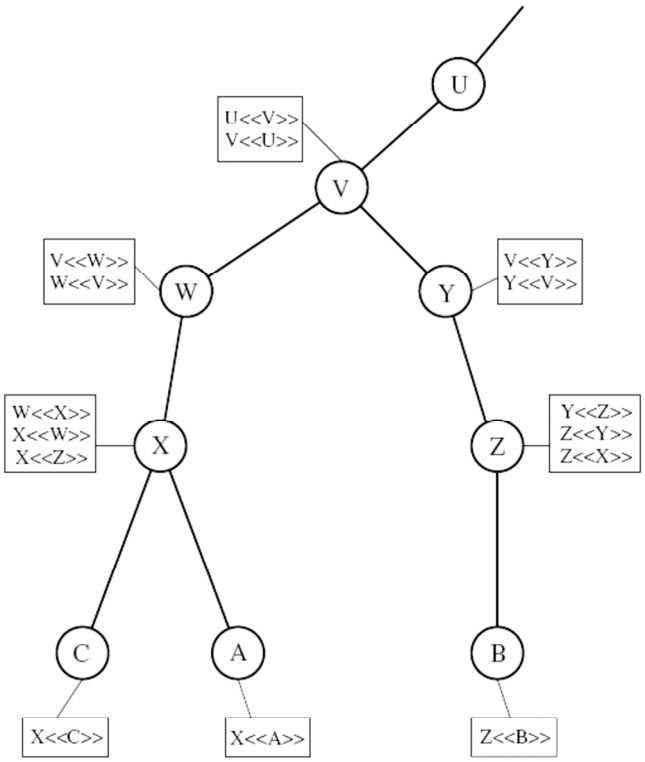

Figura 14.5 Hierarquia X.509: um exemplo hipotético.

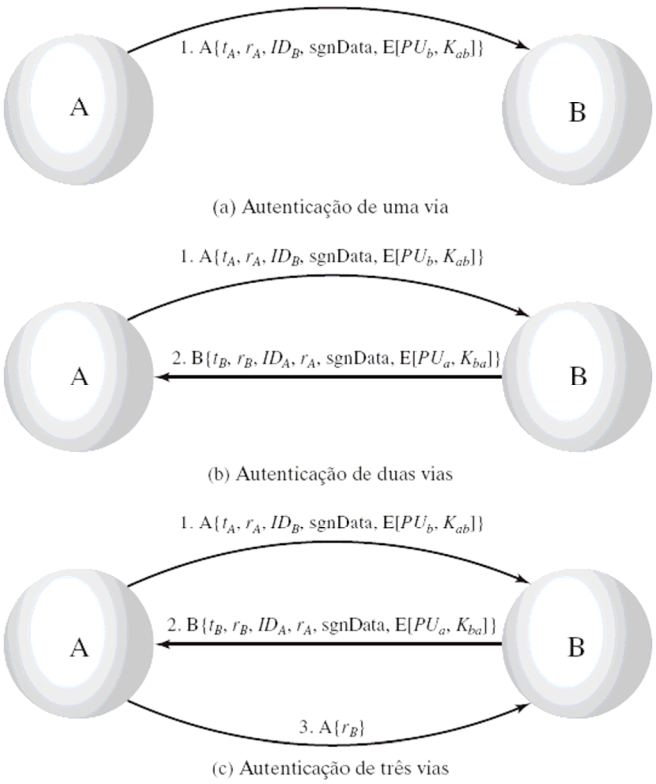

Figura 14.6 Procedimentos de autenticação forte X.509.

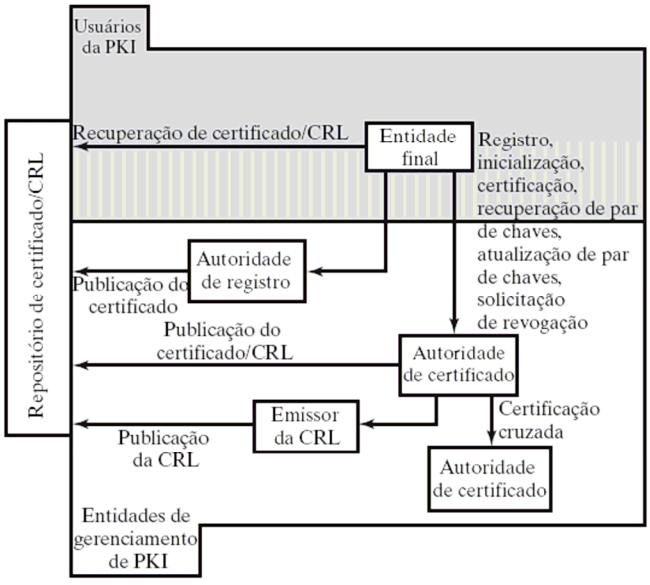

Figura 14.7 Modelo arquitetônico do PKIX.

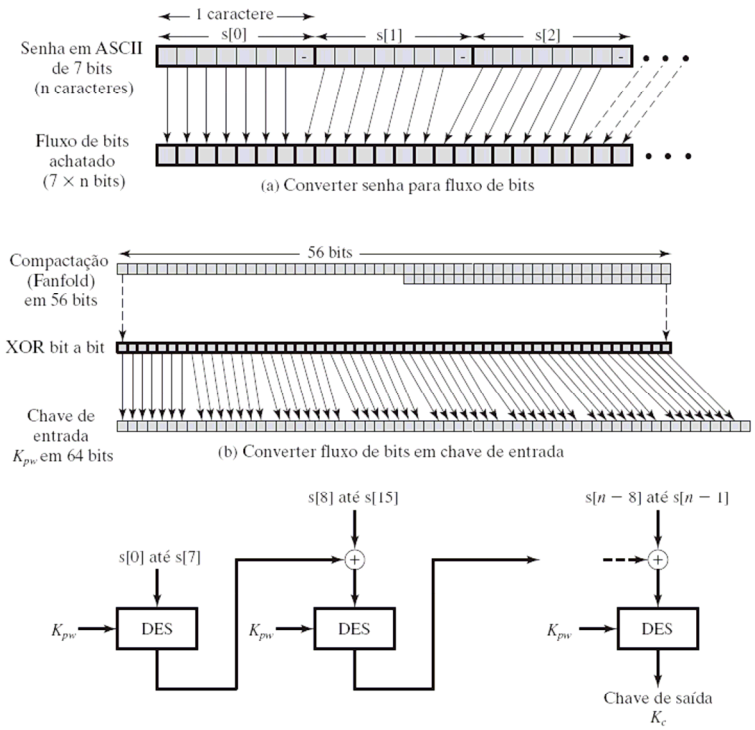

Figura 14.8 Geração de chave de criptografia a partir da senha.

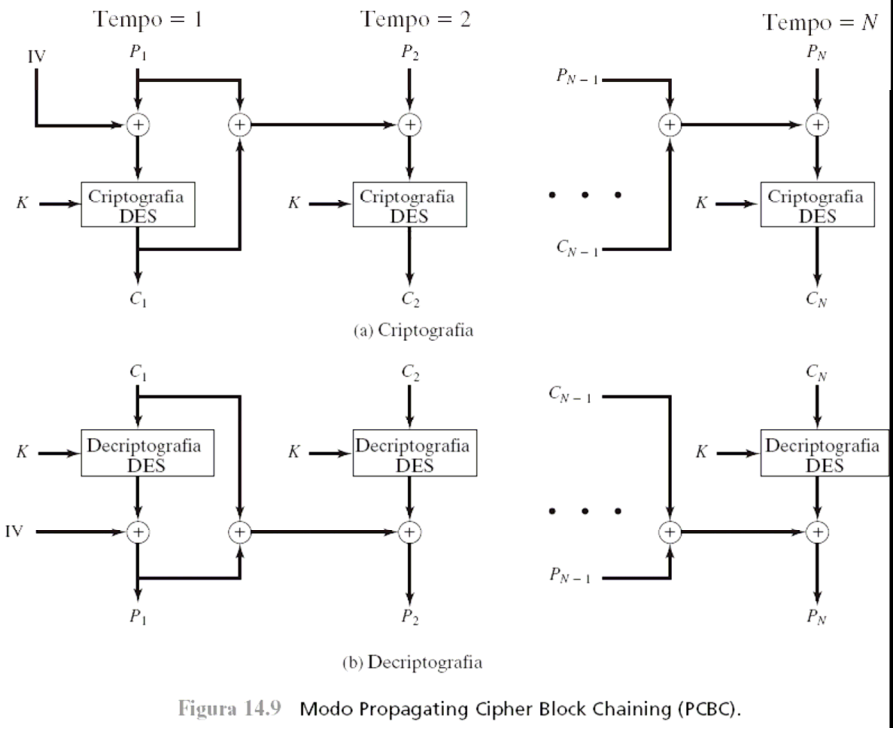

Figura 14.9 Modo Propagating Cipher Block Chaining (PCBC).