ACH 2147 — Desenvolvimento de Sistemas de Informação Distribuídos

Aula 27: Segurança (parte 1)

Prof. Renan Alves

Escola de Artes, Ciências e Humanidades — EACH — USP

17/06/2024

Introdução à segurança

Noções básicas

Um sistema confiável (dependable) provê disponibilidade, confiabilidade, segurança (safety), manutenibilidade, confidencialidade e integridade.

- Confidencialidade: refere-se à propriedade de que a informação é divulgada apenas para partes autorizadas.
- Integridade: alterações nos ativos de um sistema só podem ser feitas de maneira autorizada, garantindo precisão e completude.

Introdução à segurança

Noções básicas

Um sistema confiável (dependable) provê disponibilidade, confiabilidade, segurança (safety), manutenibilidade, confidencialidade e integridade.

- Confidencialidade: refere-se à propriedade de que a informação é divulgada apenas para partes autorizadas.
- Integridade: alterações nos ativos de um sistema só podem ser feitas de maneira autorizada, garantindo precisão e completude.

Visão alternativa

Tentamos nos proteger contra ameaças à segurança:

1. Divulgação não autorizada de informações (confidencialidade)
2. Modificação não autorizada de informações (integridade)
3. Negação de uso não autorizada (disponibilidade)

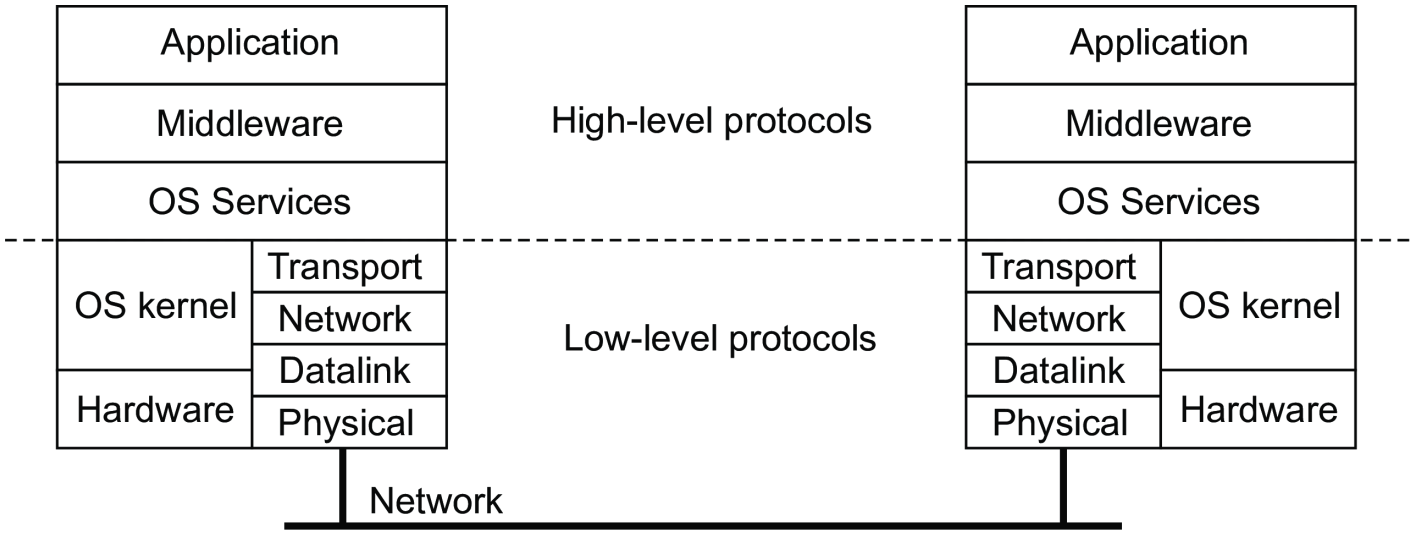
Mecanismos de segurança

- Cifração: transformar dados em algo que um atacante não possa entender, ou que possa ser verificado se foi modificado.
- Autenticação: verificar se uma identidade é verdadeira.
- Autorização: verificar se uma entidade autenticada possui os direitos adequados para acessar recursos.
- Monitoramento e auditoria: rastrear (continuamente) o acesso aos recursos.

Princípios básicos de segurança

- Valores padrão não-triviais: os padrões devem fornecer boa proteção desde o início. Exemplo infame: senha padrão "*admin*/*admin*".
- Design aberto: não usar segurança por obscuridade: todo aspecto de um sistema distribuído deve estar disponível para revisão.
- Separação de privilégios: garantir que aspectos críticos de um sistema nunca possam ser totalmente controlados por uma única entidade.
- Privilégio mínimo: um processo deve operar com a menor quantidade possível de privilégios.
- Mecanismo comum: se vários componentes requerem o mesmo mecanismo, então todos devem receber a mesma implementação desse mecanismo.

Onde implementar mecanismos de segurança?



Observação

Segurança fim-a-fim é cada vez mais comum, o que significa que os mecanismos são implementados no nível de aplicação.

Sobre privacidade

Observação

Privacidade e confidencialidade estão intimamente relacionadas, porém diferentes. Privacidade pode ser invadida, enquanto confidencialidade pode ser violada $\Rightarrow$ garantir confidencialidade não é suficiente para garantir privacidade.

Sobre privacidade

Observação

Privacidade e confidencialidade estão intimamente relacionadas, porém diferentes. Privacidade pode ser invadida, enquanto confidencialidade pode ser violada $\Rightarrow$ garantir confidencialidade não é suficiente para garantir privacidade.

Direito à privacidade

O direito à privacidade é sobre "um direito ao fluxo adequado de informações pessoais". Controle sobre quem pode ver o quê, quando e como $\Rightarrow$ uma pessoa deve ser capaz de interromper e revogar o fluxo de informações pessoais.

Sobre privacidade

Observação

Privacidade e confidencialidade estão intimamente relacionadas, porém diferentes. Privacidade pode ser invadida, enquanto confidencialidade pode ser violada $\Rightarrow$ garantir confidencialidade não é suficiente para garantir privacidade.

Direito à privacidade

O direito à privacidade é sobre "um direito ao fluxo adequado de informações pessoais". Controle sobre quem pode ver o quê, quando e como $\Rightarrow$ uma pessoa deve ser capaz de interromper e revogar o fluxo de informações pessoais.

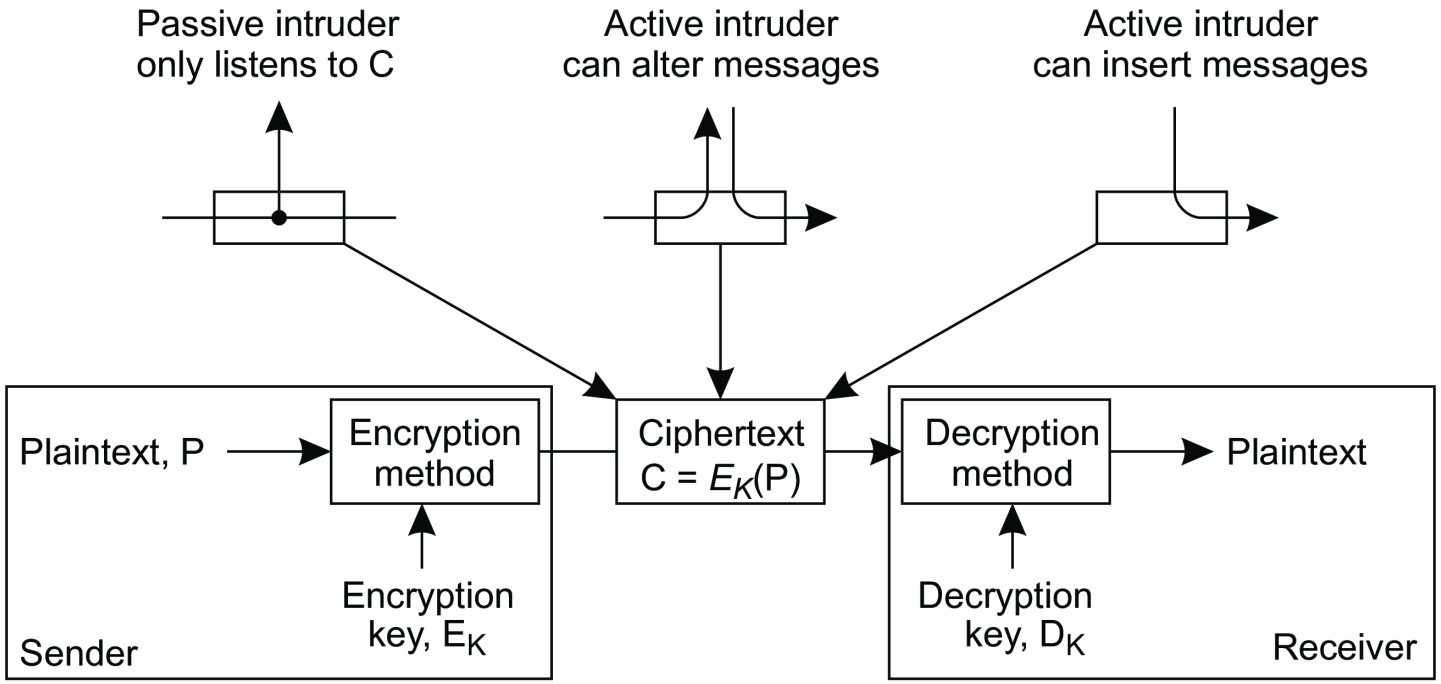
Lei Geral de Proteção de Dados (LGPD)

Lei brasileira que visa proteger os dados pessoais.

LGPD: princípios

Finalidade	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
Necessidade	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
Livre acesso	Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
Qualidade dos dados	Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.
Transparência	Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.
Segurança	Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
Prevenção	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
Não discriminação	Impossibilidade de realização do tratamento dos dados para fins discriminatórios ilícitos ou abusivos

Criptografia



Conceitos básicos

- Texto claro (plaintext): a mensagem ou os dados originais (P)
- Texto cifrado: a versão criptografada do texto claro (C)
- Chave de cifração: entrada E_K para uma função de cifração: $C = E_K(P)$
- Chave de decifração: entrada D_K para uma função de decifração: $P = D_K(C)$

Criptossistemas

Simétrico : *se* $P = D_K(E_K(P))$ *então* $D_K = E_K$.

Assimétrico : *se* $P = D_K(E_K(P))$ *então* $D_K \neq E_K$.
Também chamados de sistemas de chave pública com uma chave publicamente conhecida PK e chave secreta SK

Exemplos

Seja PK_X a chave pública de X e SK_X a chave secreta associada.

Mensagem confidencial : *se m deve ser mantida privada:* $C = PK_{receptor}(m)$.

Mensagem autenticada : *se m deve ser autenticada:* $C = SK_{remetente}(m)$.

Criptografia homomórfica

Operações matemáticas no texto claro podem ser realizadas no texto cifrado correspondente: se x e y são dois números, então

$$E_K(x) \star E_K(y) = E_K(x * y)$$

Funções hash

Descrição

Uma função hash *H* recebe uma mensagem *m* de comprimento arbitrário como entrada e produz uma sequência de bits *h* de comprimento fixo como saída:

$$h = H(m) \text{ o comprimento de } h \text{ sendo constante.}$$

Propriedades necessárias

- Direção única: dado um hash h, é inviável encontrar m tal que h = H(m)
- Resistência a colisão fraca: dado um hash h = H(m), é inviável encontrar m' tal que h = H(m')
- Resistência a colisão forte: dado uma função de hash H, é inviável encontrar m e m' tal que H(m) = H(m')

Assinatura digital

Alice calcula um resumo de m; criptografa o resumo com sua chave privada; o resumo criptografado é enviado junto com m para Bob:

$$\text{Alice: } \textit{envia } [m, sig] \textit{ com } sig = SK_A(H(m)).$$

Bob descriptografa o resumo com a chave pública de Alice; calcula separadamente o resumo da mensagem. Se ambos coincidirem, Bob sabe que a mensagem foi assinada por Alice:

$$\text{Bob: } \textit{recebe } [m, sig], \textit{ calcula } h' = H(m) \textit{ e verifica } h' = PK_A(sig).$$

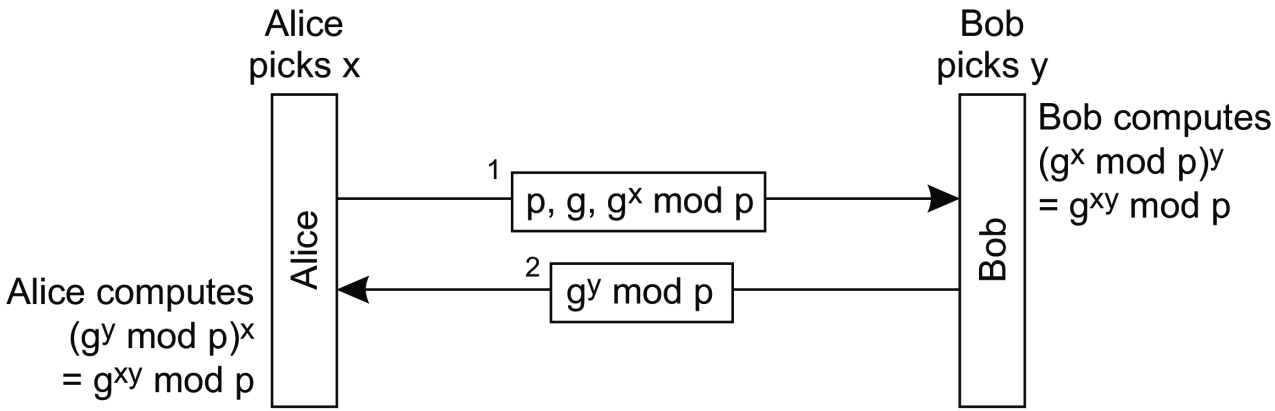
Gerenciamento de chaves

Essência

Como Alice e Bob obtêm as chaves corretas (geralmente compartilhadas) para que possam estabelecer canais seguros?

Troca de chaves Diffie-Hellman

Assuma dois números grandes, não secretos, *p* e *g* (com propriedades matemáticas específicas):



Transferência inconsciente

Transferência inconsciente: definição

Alice tem n mensagens secretas $m_1, \ldots, m_n$. Bob está interessado em (e tem permissão para) saber apenas a mensagem m_i. Qual mensagem ele quer saber deve ser mantida em segredo para Alice; todas as mensagens $m_j \neq m_i$ devem ser mantidas em segredo para Bob.

Transferência inconsciente

Transferência inconsciente: definição

Alice tem n mensagens secretas $m_1, \ldots, m_n$. Bob está interessado em (e tem permissão para) saber apenas a mensagem m_i. Qual mensagem ele quer saber deve ser mantida em segredo para Alice; todas as mensagens $m_j \neq m_i$ devem ser mantidas em segredo para Bob.

Transferência inconsciente

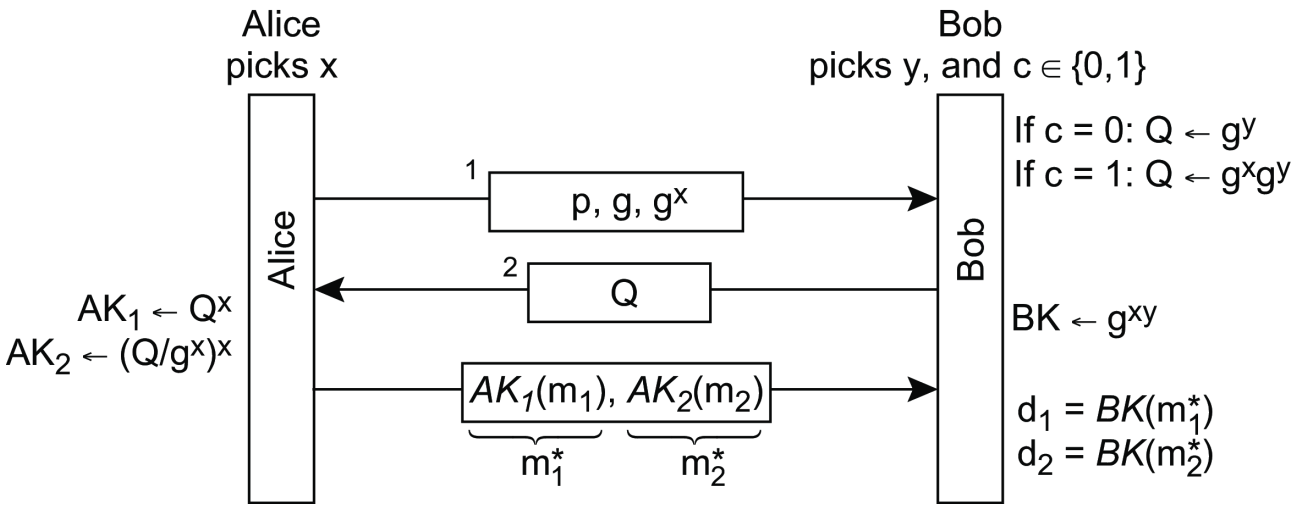
Transferência inconsciente: definição

Alice tem n mensagens secretas $m_1, \ldots, m_n$. Bob está interessado em (e tem permissão para) saber apenas a mensagem m_i. Qual mensagem ele quer saber deve ser mantida em segredo para Alice; todas as mensagens $m_j \neq m_i$ devem ser mantidas em segredo para Bob.

Solução

Bob gera um número Q que Alice, por sua vez, usa para gerar n diferentes chaves de cifração $PK_1, \ldots, PK_n$: $m_i^* = PK_i(m_i)$
Bob usa Q para gerar uma chave de decifração SK_i que corresponde apenas PK_i. Quando Bob recebe $m_1^*, \ldots, m_n^*$ ele pode descriptografar apenas m_i^*. $SK_i(m_j^*)$ (com $i \neq j$) falhará.

Transferência inconsciente 1-de-2



Análise

- $c = 0$
  - $Q = g^y$
  - $AK_1 = BK = g^{xy}$
  - $AK_2 = g^{xy-x^2}$.
- $c = 1$
  - $Q = g^{x+y}$
  - $AK_1 = g^{x^2+xy}$
  - $AK_2 = BK = g^{xy}$.

Exemplo de uso de transferência inconsciente

Preliminares

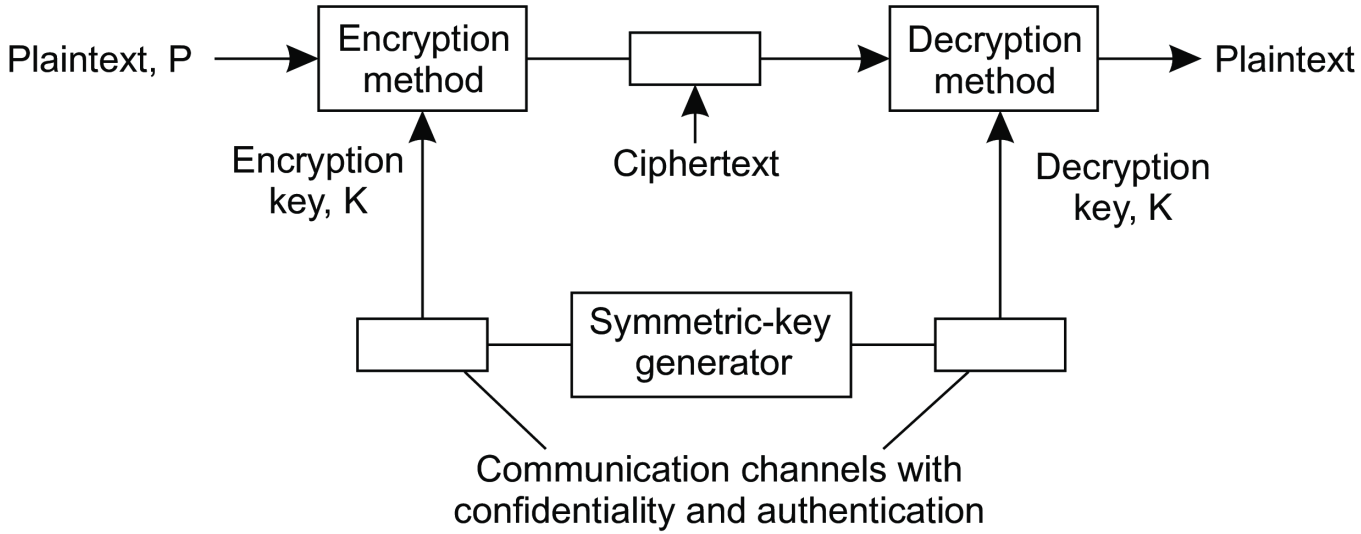
- P_1 e P_2 precisam calcular $F(a, b)$.
- O parâmetro a é secreto e conhecido apenas por P_1; o valor de b é conhecido apenas por P_2.
- $a \in \mathbf{X}$ e $b \in \mathbf{Y}$; $\mathbf{X}$ e $\mathbf{Y}$ são finitos.
- Pode-se construir uma matriz $\mathbf{F}$ de dimensões $|\mathbf{X}| \times |\mathbf{Y}|$.
- $\mathbf{F}[i, j] = F(x_i, y_j)$ para cada par $(x_i, y_j) \in \mathbf{X} \times \mathbf{Y}$.

Esboço de solução

- Cria-se $|\mathbf{X}| \cdot |\mathbf{Y}|$ pares de chaves (K_i, K_j)
- P_1 faz transferência inconsciente 1-de-$|\mathbf{X}|$.
- P_2 faz uma transferência inconsciente 1-de-$|\mathbf{Y}|$.

O que é necessário para distribuir chaves

Distribuição de chave simétrica

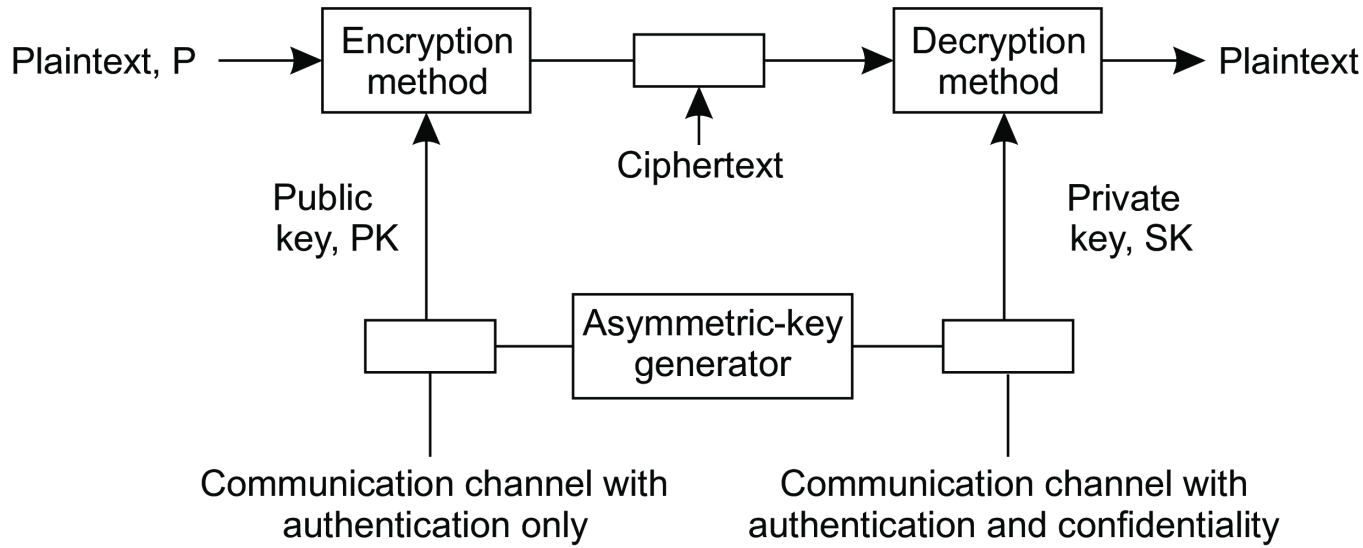


Observação

Em geral, precisaremos de um canal seguro para distribuir a chave secreta para as partes comunicantes.

O que é necessário para distribuir chaves

Distribuição de chave pública



Observação

Não há necessidade de um canal seguro no caso da chave pública, mas é necessário saber que a chave é autêntica $\Rightarrow$ ter a chave pública assinada por uma autoridade certificadora. Note que precisamos confiar nessa autoridade ou, de outra forma, garantir que sua assinatura possa ser verificada também.