Segurança da Informação

Controles de Segurança

- **CONTROLES FÍSICOS:** BARREIRAS FÍSICAS QUE IMPEDEM OU LIMITAM O ACESSO DIRETO ÀS INFORMAÇÕES OU À INFRAESTRUTURA QUE CONTÉM AS INFORMAÇÕES.

  EX: PORTAS, TRANCAS, COFRES, ALARMES, ETC.

- **CONTROLES LÓGICOS:** (CONTROLES TÉCNICOS) BARREIRAS QUE IMPEDEM OU LIMITAM O ACESSO À INFORMAÇÃO POR MEIO DE MONITORAMENTO E CONTROLE DE ACESSO.

  EX: SENHAS, FIREWALLS, CRIPTOGRAFIA, ETC.

Criptologia

- **OCULTAÇÃO DE INFORMAÇÕES:** ESTEGANOGRAFIA OU **CRIPTOGRAFIA**
  - CÓDIGOS: PALAVRAS, FRASES, SÍMBOLOS QUE SUBSTITUEM ELEMENTOS.
  - CIFRAS: ALGORITMOS DE CRIPTOGRAFIA E DESCRIPTOGRAFIA.
- **QUEBRA DOS SEGREDOS DE OCULTAÇÃO:** CRIPTOANÁLISE

Esteganografia: OCULTAR UMA MENSAGEM DENTRO DE OUTRA MENSAGEM.

Criptografia: TÉCNICA DE TORNAR UMA MENSAGEM INTELIGÍVEL.

- **PRINCIPAIS FUNDAMENTOS:**
  - SUBSTITUIÇÃO: CADA ELEMENTO É MAPEADO POR OUTRO ELEMENTO.
  - TRANSPOSIÇÃO: OS ELEMENTOS SÃO REORGANIZADOS.
- **REQUISITO ESSENCIAL:** NENHUMA INFORMAÇÃO PODE SER PERDIDA.

Princípios Fundamentais

- **CONFIDENCIALIDADE (PRIVACIDADE):** NÃO PERMITIR QUE INFORMAÇÕES ESTEJAM DISPONÍVEIS OU SEJAM ACESSADAS POR PESSOAS NÃO AUTORIZADAS.

INTEGRIDADE: GARANTIR QUE A INFORMAÇÃO MANIPULADA ESTÁ CORRETA, FIDEDIGNA, E QUE NÃO FOI CORROMPIDA (ALTERADA SEM AUTORIZAÇÃO) NO PERCURSO.

- **DISPONIBILIDADE:** GARANTIR QUE A INFORMAÇÃO ESTARÁ ACESSÍVEL E UTILIZÁVEL SOB DEMANDA POR UMA ENTIDADE **AUTORIZADA**.

Princípios Adicionais

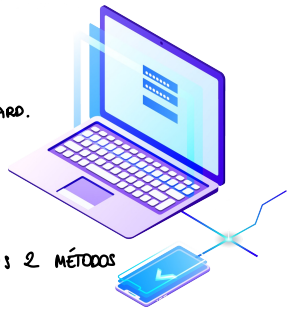
- **AUTENTICIDADE:** GARANTIR QUE O USUÁRIO EMISSOR DA MENSAGEM É DE FATO QUEM ALEGA SER.

- **IRRETRATABILIDADE:** (IRREFUTABILIDADE OU NÃO-REPÚDIO) GARANTIR QUE O EMISSOR DA MENSAGEM OU PARTICIPANTE DE UM PROCESSO NÃO NEGUE POSTERIORMENTE SUA AUTORIA.

Autenticidade

Métodos

- O QUE VOCÊ SABE? SENHAS, DADOS PESSOAIS.
- O QUE VOCÊ TEM? TOKEN, CELULAR, SMARTCARD.
- O QUE VOCÊ É? BIOMETRIA.



Autenticação Forte

- UTILIZA A COMBINAÇÃO DE PELO MENOS 2 MÉTODOS

Assinatura Digital

- É O **HASH** DA MENSAGEM CRIPTOGRAFADO COM A **CHAVE PRIVADA DO EMISSOR**, ANEXADA AO ARQUIVO, PARA PROVER:
  - INTEGRIDADE
  - NÃO-REPÚDIO.
  - AUTENTICIDADE

ASSINATURA

Criptografia Simétrica

(CHAVE DE ENCRIPTAÇÃO)

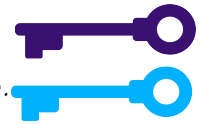
- **CRIPTOGRAFIA SIMÉTRICA:** USA UMA **CHAVE SIMÉTRICA COMPARTILHADA** TANTO P/ CODIFICAR QUANTO PARA DECODIFICAR

- GARANTE CONFIDENCIALIDADE, MAS NÃO GARANTE INTEGRIDADE E AUTENTICIDADE.
- DESVANTAGEM: O INCONVENIENTE DE TER QUE COMPARTILHAR A CHAVE.
- PRINCIPAIS ALGORITMOS: DES, 3DES, AES, BLOWFISH, CIFRAGEM DE JÚLIO CÉSAR, ETC

Criptografia Assimétrica

(CRIPTOGRAFIA DE CHAVE PÚBLICA)

- **CRIPTOGRAFIA ASSIMÉTRICA:** USA UMA **CHAVE PÚBLICA** E UMA **CHAVE PRIVADA** QUE FORMAM UM PAR EXCLUSIVO.



- GARANTE CONFIDENCIALIDADE SE:
  - EMISSOR → UTILIZA A CHAVE PÚBLICA DO DESTINATÁRIO PARA CRIPTOGRAFAR.
  - DESTINATÁRIO → UTILIZA SUA CHAVE PRIVADA PARA DESCRIPTOGRAFAR.
- GARANTE AUTENTICIDADE SE:
  - EMISSOR → UTILIZA SUA CHAVE PRIVADA PARA CRIPTOGRAFAR.
  - DESTINATÁRIO → UTILIZA A CHAVE PÚBLICA DO EMISSOR P/ DESCRIPTOGRAFAR.
- PRINCIPAIS ALGORITMOS: RSA, DSA, ECDSA, ETC.
- DESVANTAGEM: AS CHAVES SÃO MAIORES E POR ISSO A CRIPTOGRAFIA É ATÉ 100X MAIS LENTA

- **CRIPTOGRAFIA HÍBRIDA:** USA A CRIPTOGRAFIA ASSIMÉTRICA APENAS PARA TROCAR CHAVES SIMÉTRICAS (CHAVES DE SESSÃO) DE FORMA SEGURA.

- UTILIZADO POR PROTOCOLOS COMO O SSL (SECURE SOCKETS LAYER) E O TLS (TRANSPORT LAYER SECURITY)

@mapasdathai

Assinatura Digital

Algoritmo de Hash

- ALGORITMO CRIPTOGRÁFICO QUE TRANSFORMA UMA ENTRADA DE DADOS DE QUALQUER TAMANHO EM UMA SAÍDA DE DADOS DE TAMANHO FIXO.
- UMA BOA FUNÇÃO DE HASH NÃO PERMITE QUE SE DESCUBRA OS DADOS DE ENTRADA PELA ANÁLISE DOS DADOS DA SAÍDA.
- DIFERENTES ENTRADAS PODEM GERAR A MESMA SAÍDA → COLISÃO.
- P/ REDUZIR O RISCO DE COLISÃO → AUMENTA-SE O TAMANHO FIXO DE SAÍDA (PELO MENOS 128 BITS).
- USA CHAVES ASSIMÉTRICAS: O EMISSOR USA SUA CHAVE PRIVADA P/ ENCRIPTAR E O RECEPTOR USA A CHAVE PÚBLICA DO EMISSOR P/ DECRIPTAR O HASH.

Observações Gerais

GARANTE:

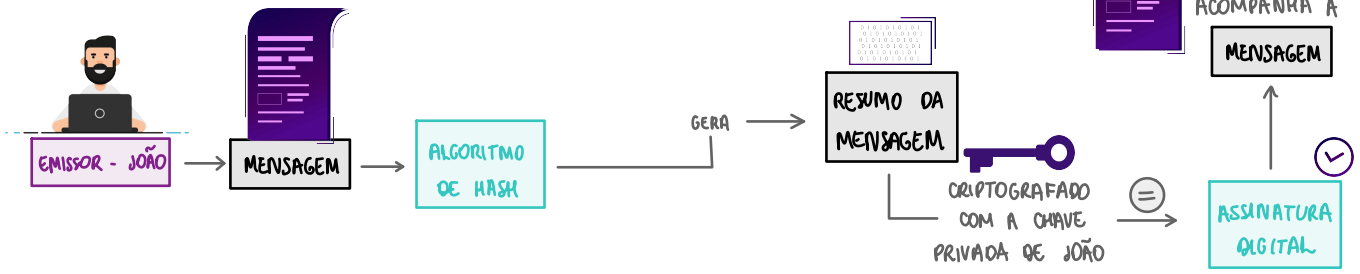
- INTEGRIDADE: UTILIZANDO O ALGORITMO DE HASH;
- NÃO-REPÚDIO: COMBINANDO INTEGRIDADE E AUTENTICIDADE;
- AUTENTICIDADE: CRIPTOGRAFANDO COM A CHAVE PRIVADA.

ASSINATURA

- NÃO GARANTE CONFIDENCIALIDADE!
  - ↳ NÃO CRIPTOGRAFA O CONTEÚDO DA MENSAGEM
- PRINCIPAIS ALGORITMOS: SHA-1 (HASH DE 160bits), MD5 (HASH DE 128bits), ETC.

Passo a Passo do Algoritmo de Hash

1. MENSAGEM É ESCRITA PELO EMISSOR;
2. CÁLCULO DO HASH DA MENSAGEM P/ GARANTIR INTEGRIDADE;
3. HASH ENCRIPTADO (COM A CHAVE PRIVADA DO EMISSOR) = ASSINATURA DIGITAL;
4. MENSAGEM ASSINADA DIGITALMENTE É TRANSMITIDA POR UM CANAL DE COMUNICAÇÃO;
5. MENSAGEM RECEBIDA E LEGÍVEL (NÃO HÁ CONFIDENCIALIDADE);
6. HASH DECRIPTADO (COM A CHAVE PÚBLICA DO EMISSOR);
7. CÁLCULO DO HASH DA MENSAGEM RECEBIDA;
8. HASH DECRIPTADO CONFRONTADO COM O HASH DA MENSAGEM RECEBIDA PARA VERIFICAÇÃO DE INTEGRIDADE;
9. SE OS HASHS FOREM IGUAIS → MENSAGEM AUTÊNTICA, ÍNTEGRA E IRREFUTÁVEL.



@mapasdathai

Certificado Digital

Conceito

- DOCUMENTO ELETRÔNICO ASSINADO DIGITALMENTE POR UMA TERCEIRA PARTE CONFIÁVEL (AUTORIDADE CERTIFICADORA) E QUE CUMPRE A FUNÇÃO DE ASSOCIAR UMA ENTIDADE (PESSOA, PROCESSO, SERVIDOR, ETC) A UM PAR DE CHAVES CRIPTOGRÁFICAS COM O INTUITO DE TORNAR AS COMUNICAÇÕES MAIS CONFIÁVEIS.

Autoridade Certificadora Raiz

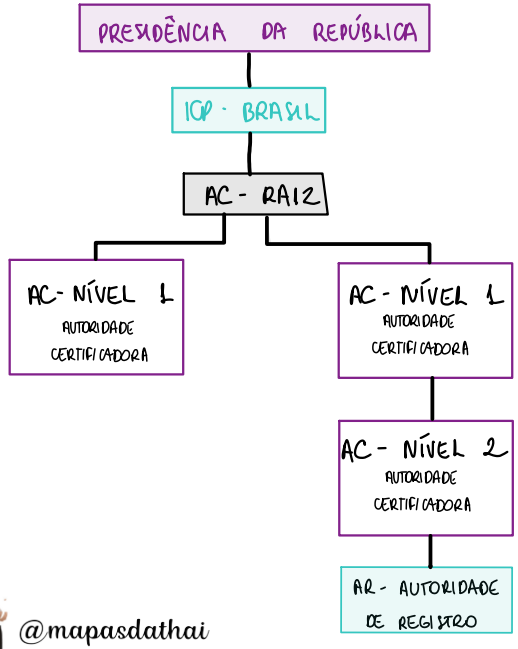
- PRIMEIRA AUTORIDADE NA CADEIA DE CERTIFICAÇÃO;
- EXECUTA AS POLÍTICAS E NORMAS DEFINIDAS PELO ICP-BRASIL;
- EMITE, EXPEDE, DISTRIBUI, REVOGA E GERENCIA OS CERTIFICADOS DAS AUTORIDADES CERTIFICADORAS DE NÍVEIS SUBSEQUENTES;
  EMITE A LCR (LISTA DE CERTIFICADOS REVOGADOS);
  FISCALIZA E AUDITA AS ACs, AS ARs E OUTRAS PRESTADORAS DE PERVIÇO HABILITADAS NA ICP-BRASIL.

Autoridade Certificadora

- EMITE, DISTRIBUI, RENOVA, REVOGA E GERENCIA CERTIFICADOS DIGITAIS;
- BUSCA VERIFICAR SE O TITULAR DO CERTIFICADO POSSUI A CHAVE PRIVADA QUE CORRESPONDE À CHAVE PÚBLICA DO CERTIFICADO;
- CRIA E ASSINA DIGITALMENTE O CERTIFICADO DO ASSINANTE;
- EMITE A LCR;
  MANTÉM REGISTRO DE SUAS OPERAÇÕES;
- ESTABELECE E FAZ AS ARs A ELA VINCULADAS CUMPRIREM AS POLÍTICAS DE SEGURANÇA P/ GARANTIR A AUTENTICIDADE DA IDENTIFICAÇÃO.

Infraestrutura de Chave Pública (ICP Brasil)

- ENTIDADE QUE MANTÉM UMA ESTRUTURA DE EMISSÃO DE CHAVES PÚBLICAS;
- TERCEIRA PARTE CONFIÁVEL;
- É QUEM EMITE O CERTIFICADO DIGITAL DA AUTORIDADE CERTIFICADORA;
- DEFINE UM CONJUNTO DE TÉCNICAS, PRÁTICAS E PROCEDIMENTOS A SEREM ADOTADOS PELAS ENTIDADES;
- ICP-BRASIL = AUTORIDADES CERTIFICADORAS + AUTORIDADES DE REGISTRO.



Autoridade de Registro

- É RESPONSÁVEL PELA INTERFACE ENTRE O USUÁRIO E A AUTORIDADE CERTIFICADORA;
- É VINCULADA A UMA AC;
- RECEBE, VALIDA E ENCAMINHA SOLICITAÇÃO DE EMISSÃO OU REVOGAÇÃO DE CERTIFICADOS;
- IDENTIFICA, DE FORMA PRESENCIAL, OS SOLICITANTES;
- MANTÉM REGISTRO DE SUAS OPERAÇÕES.

AS ARs NÃO EMITEM CERTIFICADOS!

Tipos de Certificado

- CERTIFICADOS DE ASSINATURA DIGITAL (A): CONFIRMAÇÃO DE IDENTIDADE NA WEB, EM E-MAILS, EM VPNs E DOCUMENTOS ELETRÔNICOS

CERTIFICADOS DE SIGILO (S): CODIFICAÇÃO DE DOCUMENTOS, DE BASES DE DADOS E OUTRAS INFORMAÇÕES SIGILOSAS.

TIPO	GERAÇÃO DO PAR DE CHAVES	TAMANHO MÍNIMO	ARMAZENAMENTO	VALIDADE (ANOS)
A1 / S1	SOFTWARE	1024 BITS	DISCO RÍGIDO (HD) E PENDRIVE	1
A2 / S2	SOFTWARE	1024 BITS	SMARTCARD OU TOKEN USB	2
A3 / S3	HARDWARE	1024 BITS	SMARTCARD OU TOKEN USB	5
A4 / S4	HARDWARE	2048 BITS	SMARTCARD OU TOKEN USB	6

@mapasdathai