Documentação das Tentativas de Geração de Chaves RSA - Projeto Criptografia Híbrida

Usuária: Andrea

Ambiente: Linux, OpenSSL 3.5.0, PHP 8.4.8

Diretório das chaves: /srv/http/bcs-expcriativa3/keys/

Histórico de Comandos e Resultados

1. Tentativas com formatos incorretos (OpenSSH)

- **Comando utilizado**: `bash openssl genpkey -algorithm RSA -out private.pem -pkeyopt rsa_keygen_bits:2048 openssl rsa -pubout -in private.pem -out public.pem`
- **Resultado**: `private.pem: OpenSSH private key (no password) public.pem: OpenSSH public key`
- **Problema**: O PHP não reconhece chaves em formato OpenSSH. Necessário formato PEM RSA tradicional (PKCS#1).

---

2. Tentativas com PKCS#8 (ainda incompatível)

- **Comando**: `bash openssl genpkey -algorithm RSA -out private.pem`
- **Validação**: `head -n 1 private.pem => -----BEGIN PRIVATE KEY-----`
- **Problema**: PKCS#8 detectado (`-----BEGIN PRIVATE KEY-----`). PHP `openssl_private_decrypt` requer PKCS#1 (`-----BEGIN RSA PRIVATE KEY-----`).

---

3. Tentativa correta (PKCS#1)

- **Comando utilizado**: `bash openssl genrsa -out private.pem 2048 openssl rsa -in private.pem -pubout -out public.pem`

- **Validação**: `head -n 1 private.pem => -----BEGIN RSA PRIVATE KEY----- head -n 1 public.pem => -----BEGIN PUBLIC KEY-----`

- **Status**: Arquivos no formato correto!
-

---

4. Testes com `testa_chave.php`

- **Resultado esperado**: `Chave privada carregada com sucesso.`
- **Status**: Sucesso na leitura com `openssl_pkey_get_private()`.

---

5. Erros posteriores

- **Erro persistente**: `Erro ao descriptografar a chave AES.`
- **Causa provável**: JS está codificando/enviando com chave pública incompatível com a privada.

Conclusão

A geração correta foi com:

```
bash sudo openssl genrsa -out private.pem 2048 sudo openssl rsa -in private.pem -pubout -out public.pem
```

E confirmação de: - `private.pem`: deve iniciar com `-----BEGIN RSA PRIVATE KEY-----` - `public.pem`: deve iniciar com `-----BEGIN PUBLIC KEY-----`

Documento gerado em: 22/06/2025 15:10:53