证其是否匹配。如果客户端反过来用客户端随机数对服务器进行质询，就会创建客户端摘要。服务器可以预先将下一个随机数计算出来，提前将其传递给客户端，这样下一次客户端就可以预先发送正确的摘要了。

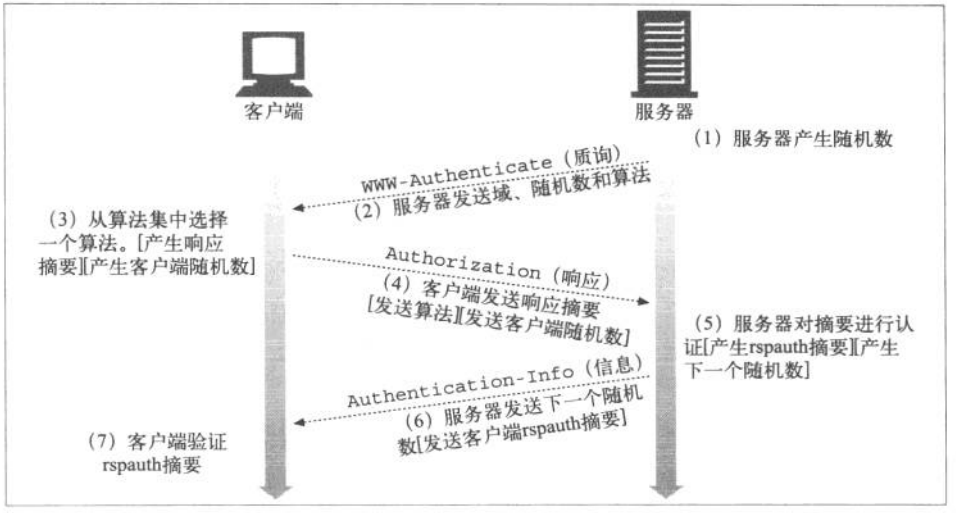

图 13-2 摘要认证的握手机制

这些信息中很多是可选的，而且有默认值。为了说明问题，图 13-3 对比了基本认证中发送的报文（参见图 13-3a 至图 13-3d）与简单的摘要认证实例发送的报文（参见图 13-3e 至图 13-3h）。

现在我们来更详细地探讨摘要认证的内部工作原理。

13.2 摘要的计算

摘要认证的核心就是对公共信息、保密信息和有时限的随机值这个组合的单向摘要。现在我们来看看这些摘要是如何计算出来的。摘要计算通常都是简单易懂的。[10] 附录 F 提供了示例源代码。

13.2.1 摘要算法的输入数据

摘要是根据以下三个组件计算出来的。

- 由单向散列函数 H(*d*) 和摘要 KD(*s*,*d*) 组成的一对函数，其中 *s* 表示密码，*d* 表示数据。

注 10：但对初学者来说，可选的 RFC 2617 兼容模式以及规范中背景资料的缺乏，使其变得有些复杂。我们会努力提供一些帮助。