- 一个包含了安全信息的数据块，包括密码，称为 A1。
- 一个包含了请求报文中非保密属性的数据块，称为 A2。

H 和 KD 处理两块数据 A1 和 A2，产生摘要。

13.2.2 算法H(*d*)和KD(*s*,*d*)

291 ~ 292

摘要认证支持对各种摘要算法的选择。RFC 2617 建议的两种算法为 MD5 和 MD5-sess（“sess”表示会话），如果没有指定其他算法，默认算法为 MD5。

不管使用的是 MD5 还是 MD5-sess，都会用函数 H 来计算数据的 MD5，用摘要函数 KD 来计算以冒号连接的密码和非保密数据的 MD5。例如：

```
H(<data>) = MD5(<data>)
KD(<secret>,<data>) = H(concatenate(<secret>:<data>))
```

13.2.3 与安全性相关的数据（A1）

被称为 A1 的数据块是密码和受保护信息的产物，它包含有用户名、密码、保护域和随机数等内容。A1 只涉及安全信息，与底层报文自身无关。A1 会与 H、KD 和 A2 一同用于摘要计算。

RFC 2617 根据选择的算法定义了两种计算 A1 的方式。

- MD5

为每条请求运行单向散列函数。A1 是由冒号连接起来的用户名、域以及密码三元组。

- MD5-sess

只在第一次 `WWW-Authenticate` 握手时运行一次散列函数。对用户名、域和密码进行一次 CPU 密集型散列，并将其放在当前随机数和客户端随机数（cnonce）的前面。

表 13-2 显示了 A1 的定义。

表13-2 算法对A1的定义

算法	A1
MD5	`A1 = <user>:<realm>:<password>`
MD5-sess	`A1 = MD5(<user>:<realm>:<password>):<nonce>:<cnonce>`

13.2.4 与报文有关的数据（A2）

数据块 A2 表示的是与报文自身有关的信息，比如 URL、请求方法和报文实体的主