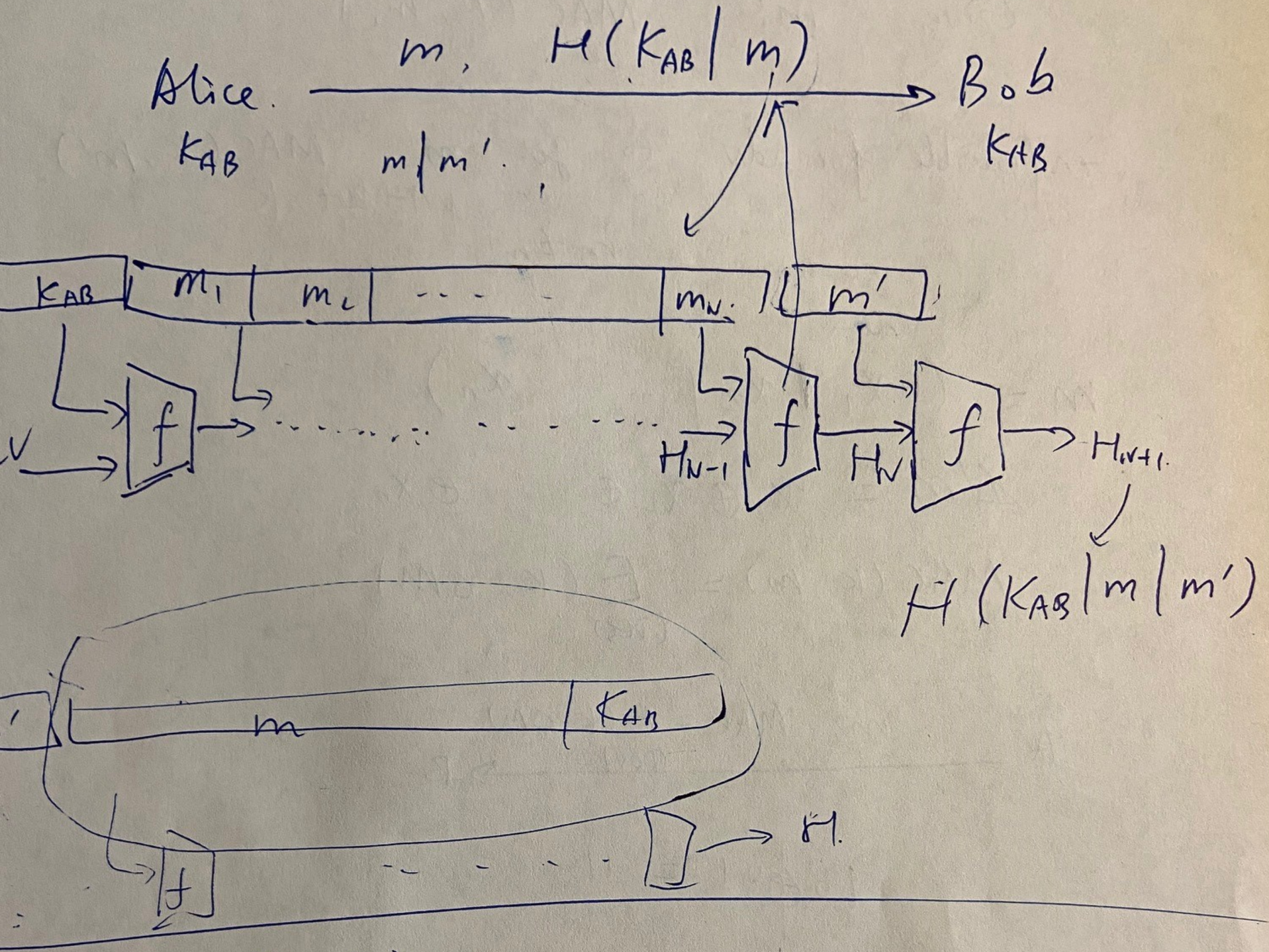
2/24/2021

Message Authentication Codes.



HMAC. (K, M)

$= H[(K \oplus C_2) \mid H[(K \oplus C_1) \mid M]]$

$H[(K \oplus C_2) \mid H_1]$

$H[(K \oplus C_2) \mid H_1 \mid m']$

$H[(K \oplus C_1) \mid m''] = H_1 \mid m'$

Security of MAC.

Given m_i. $MAC(K, m_i)$

infeasible for adv. to get m', $MAC(K, m')$. without K.

$m \neq m'$.

64-bits

$m = (x_1 \| x_2 | \cdots \cdots x_n)$.

$\Delta m = x_1 \oplus x_2 \oplus \cdots \cdots \oplus x_n$

$MAC(K, m) = \underset{(DES)}{E}(K, \Delta M)$

A $\xrightarrow[(DES)]{m,\ MAC = E(K, \Delta M)}$ B

$1001 = 11$

↓

$0101 = 11$.

---

x_4

$1111 \nearrow 0$.

$\oplus\ 1001$

$0111 \nearrow 1$.

$\oplus\ 1101$ ← K

$1010 \nearrow 0$.

$x \cdots 1110\ 1010$

$1111\ 1011$

✗ ① $C = E(K, m)$ $A \longrightarrow B$ (A: K, B: K)

$C \rightarrow C'$

$dec \rightarrow m'$

✓ ② $A \xrightarrow{C = E(K, M \| 10000\ldots)} B$

$C \rightarrow C'$

$dec \rightarrow m' \| 0101\ldots$

2^{-80}

✓ ③ $A \xrightarrow{E(K, M | C(m))} B$

low prob.

$c \rightarrow c'$

$m' | c'$

✗ ④ $y = E(K, m)$, $C(y)$ $\longrightarrow B$

$y' \rightarrow C(y')$

✓ ⑤ M . $MAC(K, m)$ $\longrightarrow$ HMAC.

✓ integrity

✗ confid.

✓ ⑥ $E(K, m \| MAC(K, m))$ $\longrightarrow$

2/24/2021 Hash Applications

Authenticated Encryption (AE)

① hash then Encryt.

$E(K, M \| H(M))$ ✗ WEP. (wifi)

② Authen → Enc A → E

$E(K_2, M \| MAC(K_1, M))$ two keys

HMAC SSL/TLS.

✓ theoretical secure.

③ Enc. → Authen E → A.

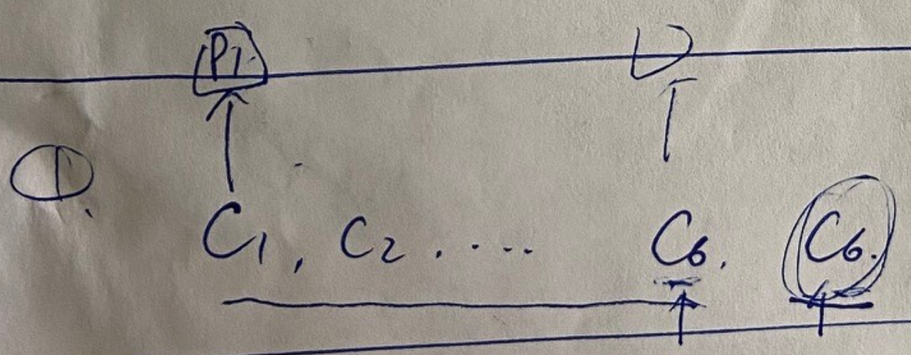
✓ $C = E(K_2, M)$. $MAC(K_1, C)$

IPSec.

④ Enc + Authen.

$C = E(K_2, M)$. ⊕ $MAC(K_1, M)$

SSH/telnet



H(pwd). dictionary attack.