62

O que é segurança semântica (one-time)?

Um esquema é semanticamente seguro se:

- Um attacker não consegue distinguir entre cifras de duas mensagens diferentes.

- Cada mensagem deve ser cifrada com uma chave única e aleatória.

- A cifra não revela nada da mensagem.

2. $k = 0^n$

R: Logo não é semanticamente seguro pois usa sempre a mesma chave.

3. $E'(k, m) = E(k, m) \| 110$

R: É semanticamente seguro, a chave é única e aleatória, e embora ele concatene sempre 0 no final da cifra, isso não é suficiente para obter informação sobre a mensagem.

4. $E'(k, m) = E(k, m) \oplus 1^n$

R: É semantica segura pois a chave é aleatória e única, e a inversão de bits não impacta em nada a segurança desta cifra.

Digitalizada com CamScanner

6. $E'(k, m) = \underbrace{E(k, m)}_{C} \,||\, m$

C concatena mensagem original

R: Não é semanticamente seguro pois na cifra é concatenada a mensagem original, basta ao atacante ler os ultimas bits para saber a mensagem original.

§3

2.

Basta o atacante colecionar cifras suficientes para perceber que as mesmas seguem um padrão logo possuem a mesma chave.

6.

Como mencionado em cima, basta o atacante ler as ultimas bits para saber a mensagem original.

Digitalizada com CamScanner