Criptografie și Securitate

- Prelegerea 20 -
Criptarea hibridă

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

Criptarea hibridă

- Conform cu ce am văzut în anterior, criptarea unui mesaj de t biți necesită t apelări ale schemei de criptare originale;

Criptarea hibridă

- Conform cu ce am văzut în anterior, criptarea unui mesaj de t biți necesită t apelări ale schemei de criptare originale;
- Aceasta înseamnă că și calculele dar și lungimea textului criptat cresc cu un factor multiplicativ în raport cu t;

Criptarea hibridă

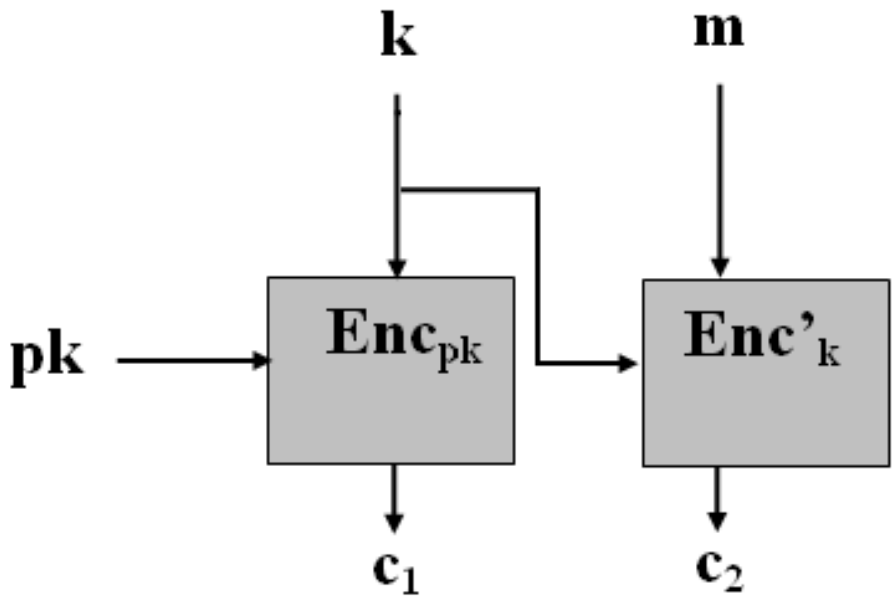
- Conform cu ce am văzut în anterior, criptarea unui mesaj de t biți necesită t apelări ale schemei de criptare originale;
- Aceasta înseamnă că și calculele dar și lungimea textului criptat cresc cu un factor multiplicativ în raport cu t;
- Pentru mesajele care sunt suficient de lungi, se folosește criptare cu cheie secretă în tandem cu criptarea cu cheie publică;

Criptarea hibridă

- Conform cu ce am văzut în anterior, criptarea unui mesaj de t biți necesită t apelări ale schemei de criptare originale;
- Aceasta înseamnă că și calculele dar și lungimea textului criptat cresc cu un factor multiplicativ în raport cu t;
- Pentru mesajele care sunt suficient de lungi, se folosește criptare cu cheie secretă în tandem cu criptarea cu cheie publică;
- Eficiența crește pentru că schemele de criptare cu cheie secretă sunt mai eficiente decât schemele de criptare cu cheie publică;

Criptarea hibridă

- Rezultatul acestei combinații se numește criptare hibridă și este folosită extensiv în practică;



Criptare hibridă

- Pentru criptarea unui mesaj m, se urmează doi pași:

Criptare hibridă

- Pentru criptarea unui mesaj m, se urmează doi pași:

1. Expeditorul alege aleator o cheie k pe care o criptează folosind cheia publică a destinatarului, rezultând $c_1 = Enc_{pk}(k)$; Numai destinatarul va putea decripta k, ea rămânând secretă pentru un adversar;

Criptare hibridă

- Pentru criptarea unui mesaj m, se urmează doi pași:

1. Expeditorul alege aleator o cheie k pe care o criptează folosind cheia publică a destinatarului, rezultând $c_1 = Enc_{pk}(k)$; Numai destinatarul va putea decripta k, ea rămânând secretă pentru un adversar;

2. Expeditorul criptează m folosind o schemă de criptare cu cheie secretă (Enc', Dec') cu cheia k, rezultând $c_2 = Enc'_k(m)$;

Criptare hibridă

- Pentru criptarea unui mesaj m, se urmează doi pași:

1. Expeditorul alege aleator o cheie k pe care o criptează folosind cheia publică a destinatarului, rezultând $c_1 = Enc_{pk}(k)$; Numai destinatarul va putea decripta k, ea rămânând secretă pentru un adversar;

2. Expeditorul criptează m folosind o schemă de criptare cu cheie secretă (Enc', Dec') cu cheia k, rezultând $c_2 = Enc'_k(m)$;

- Mesajul criptat este $c = (c_1, c_2)$;

Criptare hibridă

- Pentru criptarea unui mesaj m, se urmează doi pași:

1. Expeditorul alege aleator o cheie k pe care o criptează folosind cheia publică a destinatarului, rezultând $c_1 = Enc_{pk}(k)$; Numai destinatarul va putea decripta k, ea rămânând secretă pentru un adversar;

2. Expeditorul criptează m folosind o schemă de criptare cu cheie secretă (Enc', Dec') cu cheia k, rezultând $c_2 = Enc'_k(m)$;

- Mesajul criptat este $c = (c_1, c_2)$;

- Construcția este o schemă de criptare asimetrică (cele două părți nu partajează o cheie secretă în avans).

Criptare hibridă

- Când $|m| >> n = |k|$, criptarea hibridă oferă o îmbunătățire substanțială a eficienței față de criptarea bit cu bit sau bloc cu bloc;
- Deci, pentru mesaje suficient de lungi, ea îmbină funcționalitatea criptării cu cheie publică cu eficiența criptării cu cheie secretă.

Securitate

Teoremă

Dacă Π *este o schemă de criptare cu cheie publică CPA-sigură iar* Π' *este o schemă de criptare cu cheie secretă sigură semantic, atunci construcția hibridă* Π^{hyb} *este o schemă de criptare cu cheie publică CPA-sigură.*

Securitate

Teoremă

Dacă Π *este o schemă de criptare cu cheie publică CPA-sigură iar* Π' *este o schemă de criptare cu cheie secretă sigură semantic, atunci construcția hibridă* Π^{hyb} *este o schemă de criptare cu cheie publică CPA-sigură.*

- Este suficient ca Π' să satisfacă noțiunea mai slabă de securitate semantică (care nu implică securitate CPA)...

Securitate

Teoremă

Dacă Π *este o schemă de criptare cu cheie publică CPA-sigură iar* Π' *este o schemă de criptare cu cheie secretă sigură semantic, atunci construcția hibridă* Π^{hyb} *este o schemă de criptare cu cheie publică CPA-sigură.*

- Este suficient ca Π' să satisfacă noțiunea mai slabă de securitate semantică (care nu implică securitate CPA)...
- ...deoarece cheia secretă k este una "nouă" și aleasă aleator de fiecare dată când se criptează un mesaj;

Securitate

Teoremă

Dacă Π *este o schemă de criptare cu cheie publică CPA-sigură iar* Π' *este o schemă de criptare cu cheie secretă sigură semantic, atunci construcția hibridă* Π^{hyb} *este o schemă de criptare cu cheie publică CPA-sigură.*

- Este suficient ca Π' să satisfacă noțiunea mai slabă de securitate semantică (care nu implică securitate CPA)...
- ...deoarece cheia secretă k este una "nouă" și aleasă aleator de fiecare dată când se criptează un mesaj;
- Cum o cheie k este folosită o singură dată, e suficientă noțiunea de securitate la interceptare simplă pentru securitatea schemei hibride.

Important de reținut!

- Pentru criptarea mesajelor lungi, în practică se folosește criptarea hibridă
- Aceasta îmbină avantajele criptării simetrice și criptării asimetrice