Tài liệu tìm hiểu về mã hóa phần mềm bằng RSA

Mã hóa RSA là gì ?

Mã hóa ***RSA*** (***Rivest – Shamir – Adlemen***) sử dụng một cặp khóa (công khai – ***public*** và bí mật – ***private***) để mã hóa và giải mã dữ liệu.
Dữ liệu được mã hóa bằng khóa công khai có thể được giải mã bằng khóa bí mật tương ứng, đảm bảo tính bảo mật của thông tin.
RSA thường được ứng dụng để bảo vệ thông tin nhạy cảm, xác thực danh tính và đảm bảo tính toàn vẹn của dữ liệu trong các ứng dụng phần mềm.

Nguyên tắc hoạt động toán học

RSA thực hiện hoạt động với số nguyên tố – ***prime*** và các khái niệm liên quan như đồng nguyên tố – ***coprime***

Mối liên hệ giữa prime và coprime

1 số bất kỳ thỏa mãn là số nguyên tố – ***prime*** $\text{If}[$ thỏa mãn $\neg[$ chia hết cho bất kỳ số nào $]$ ngoài 1 và chính nó $]$
$\rightarrow$ 2 số a, b bất kỳ thỏa mãn là đồng nguyên tố – ***coprime*** $\text{If}[\ \gcd(a,b)=1\ ]$

Phi hàm Euler

Phi hàm Euler hay ***Euler's totient function***, ký hiệu $\varphi(n)$ có đầu vào là số nguyên tố n và trả về kết quả là số lượng số nguyên dương thuộc khoảng $[1;n]$ thỏa mãn ***coprime*** với số n, chính là $n-1$.
$\rightarrow$ Nghĩa là $\varphi(n)=n-1$ nếu thỏa mãn n là số nguyên tố

Trình tự thực thi

Cả 2 bên đều thực thi quy trình như sau:

1. Lựa chọn 2 số p và q bất kỳ là số nguyên tố (càng lớn càng tốt)
2. Tính tích $n=p\times q$
3. Tính phi hàm Euler của n , lúc này n không là số nguyên tố
   Ta có $\varphi(n)=\varphi(p\times q)=\varphi(p)\times\varphi(q)$
   $\rightarrow\ \varphi(n)=(p-1)\times(q-1)$
   Lúc này, p, q và $\varphi(n)$ không thể được công khai
4. Lựa chọn giá trị khóa ***public*** là e , $e\in(2;\varphi(n))$ và thỏa mãn là ***coprime*** với $\varphi(n)$
5. Lựa chọn giá trị khóa ***private*** là d thỏa mãn $(e\times d)\mod\varphi(n)=1$ (viết lại thành $e\times d\equiv 1\mod\varphi(n)$)

Phía gửi

1. Lựa chọn thông điệp m để truyền tải
2. Mã hóa thông điệp thành bản mã $c=m^e\mod n$ với e, n của phía nhận
3. Truyền tải bản mã đi

Phía nhận

1. Nhận bản mã từ phía gửi
2. Giải mã thông điệp thành bản rõ $m=c^d\mod n$

Trường hợp sử dụng chữ ký số thay thế bản mã

Phía gửi

1. Lựa chọn thông điệp m để truyền tải
2. Tính chữ ký số $s=m^d\mod n$
3. Truyền tải thông điệp và chữ ký số đi

Phía nhận

1. Nhận thông điệp từ phía gửi
2. Kiểm tra chữ ký số đảm bảo $s^e\mod n=m$