

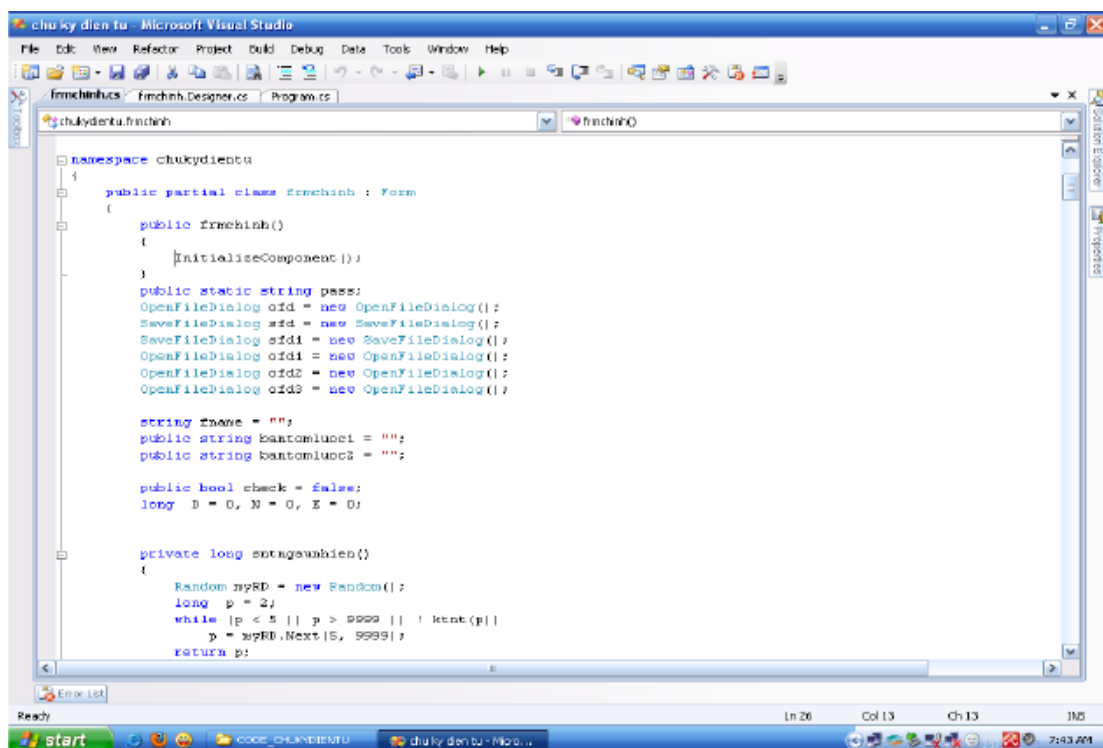
## DEMO CHƯƠNG TRÌNH CHỮ KÝ ĐIỆN TỬ

Mô tả: Đối với một văn bản trên giấy bình thường, chúng ta có thể dùng bút để ký xác nhận một cách dễ dàng. Và văn bản đó là duy nhất, không thể sửa đổi, sao chép, làm giả. (cho dù photo). Nhưng đối với một văn bản điện tử trên máy tính thì làm sao để ký xác nhận được??? Và làm thế nào để xác nhận văn bản đó không bị sửa đổi, giả mạo, đánh cắp.... trong quá trình gửi???

Chữ ký điện tử sẽ thực hiện việc cấp phép khóa (khóa bí mật: pravitakey, khóa công khai: publickey), thực hiện ký văn bản và xác nhận văn bản có đúng người gửi hay không, có bị thay đổi trong quá trình gửi hay không.

Đây là một đề tài còn khá mới, đang được phát triển và ứng dụng trong tương lai. Là đề tài làm đồ án, khóa luận rất tốt cho ngành CNTT. Sau đây là bản demo chương trình. Có gì thắc mắc hãy liên hệ với mail: [hainhat007@gmail.com](mailto:hainhat007@gmail.com) để được giải đáp!

### 1. Code



```
namespace chuky dientu
{
    public partial class Frmchinh : Form
    {
        public Frmchinh()
        {
            InitializeComponent();
        }

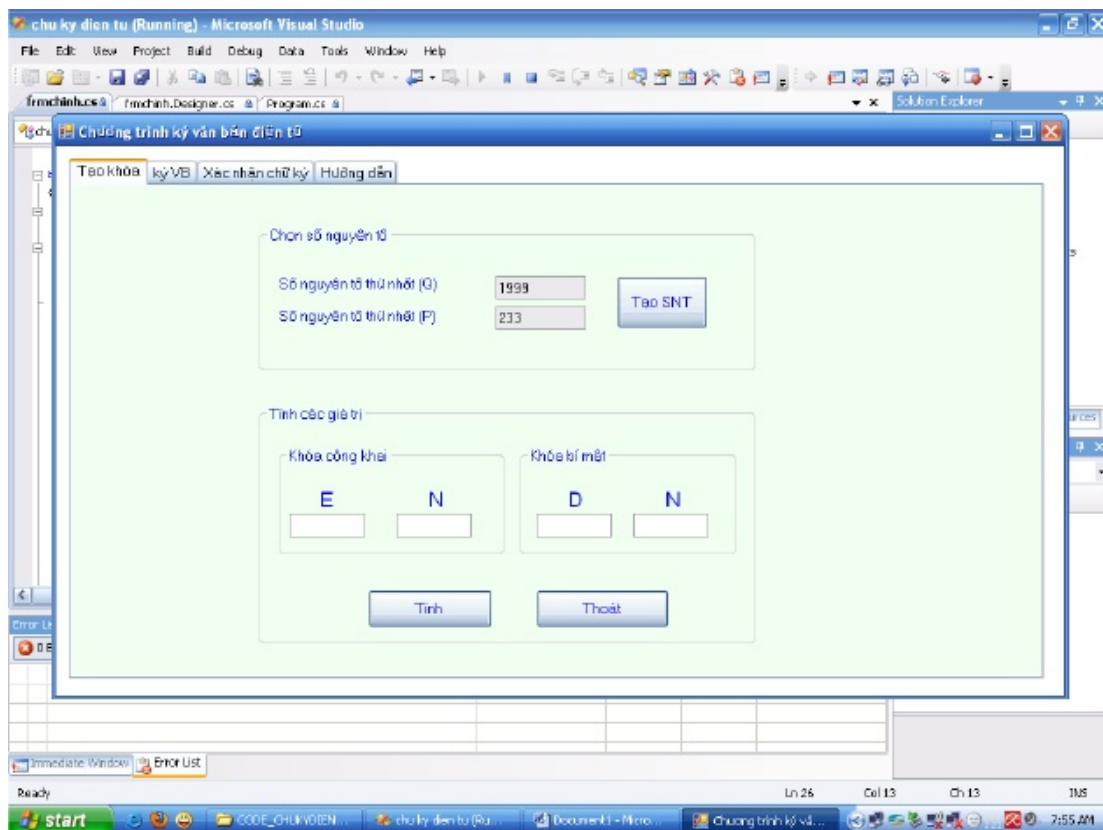
        public static string pass;
        OpenFileDialog oId = new OpenFileDialog();
        SaveFileDialog sId = new SaveFileDialog();
        SaveFileDialog sId1 = new SaveFileDialog();
        OpenFileDialog oId1 = new OpenFileDialog();
        OpenFileDialog oId2 = new OpenFileDialog();
        OpenFileDialog oId3 = new OpenFileDialog();

        string name = "";
        public string kantomluoc1 = "";
        public string kantomluoc2 = "";

        public bool check = false;
        long D = 0, N = 0, X = 0;

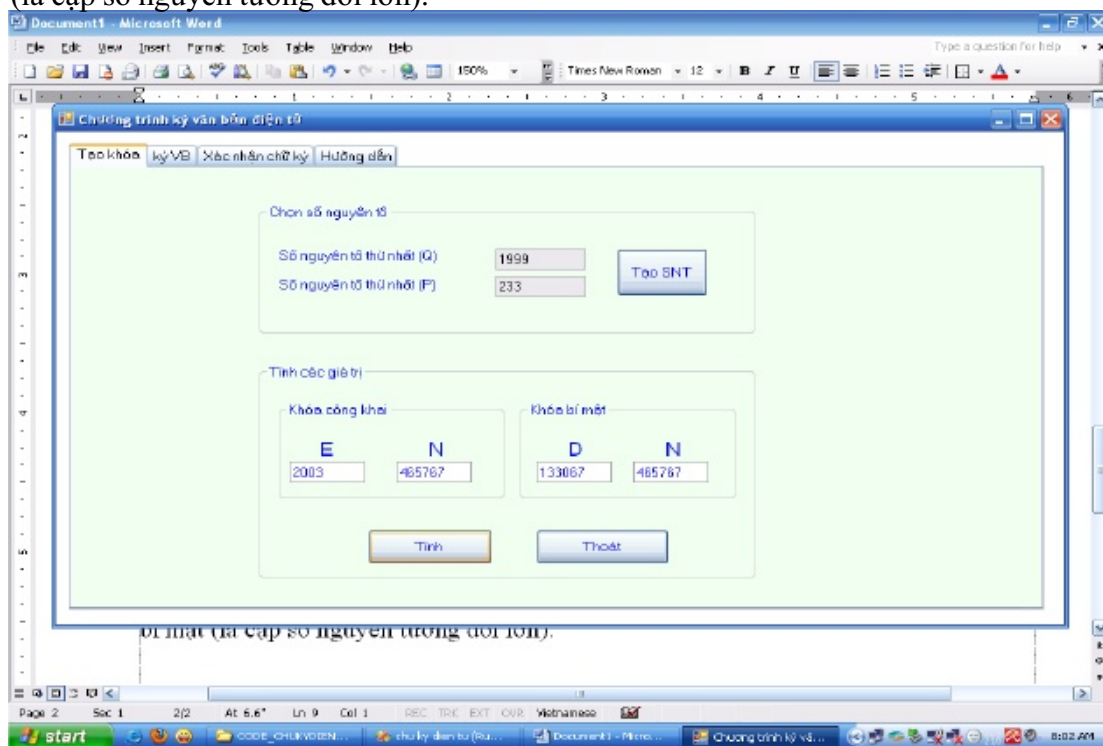
        private long sotagaukhien()
        {
            Random myRD = new Random();
            long p = 2;
            while (p < 5 || p > 9999 || !IsInt(p))
                p = myRD.Next(5, 9999);
            return p;
        }
    }
}
```

### 2. chạy ct

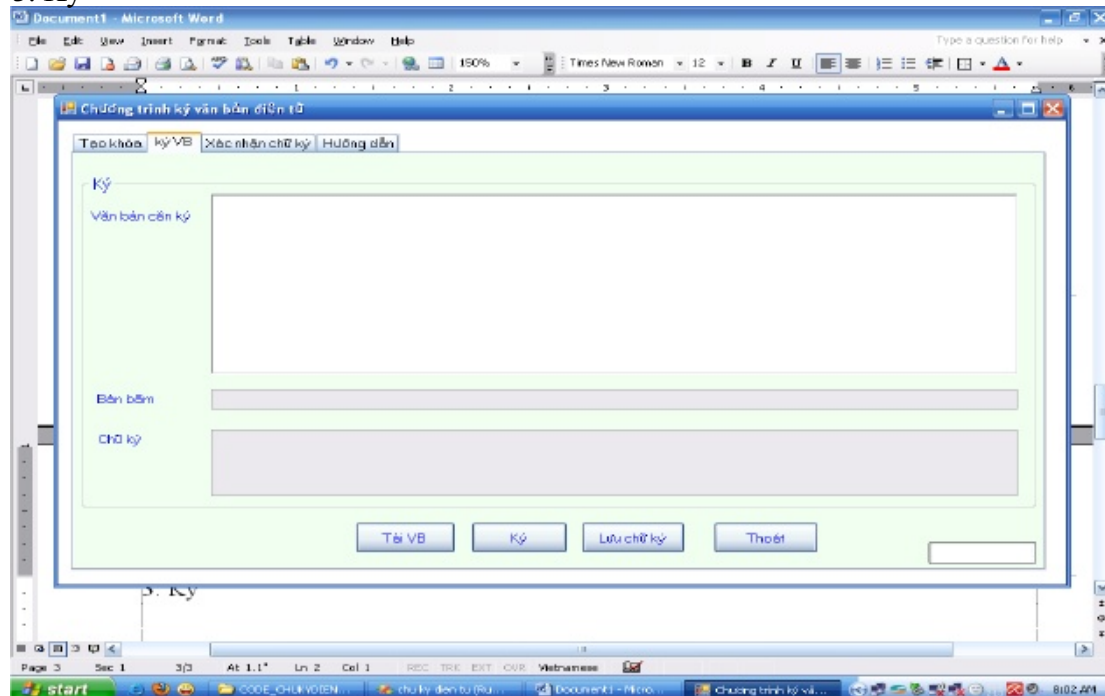


Giao tạo khóa cho phép chúng ta tạo ra cặp khóa bí mật (giữ để ký) và khóa công khai (phân phát cho tất cả mọi người để họ xác nhận chữ ký của mình). Theo thật toán RSA thì khi biết khóa công khai được phân phát thì không thể suy ra được khóa bí mật để giả mạo chữ ký (xem thêm về RSA).

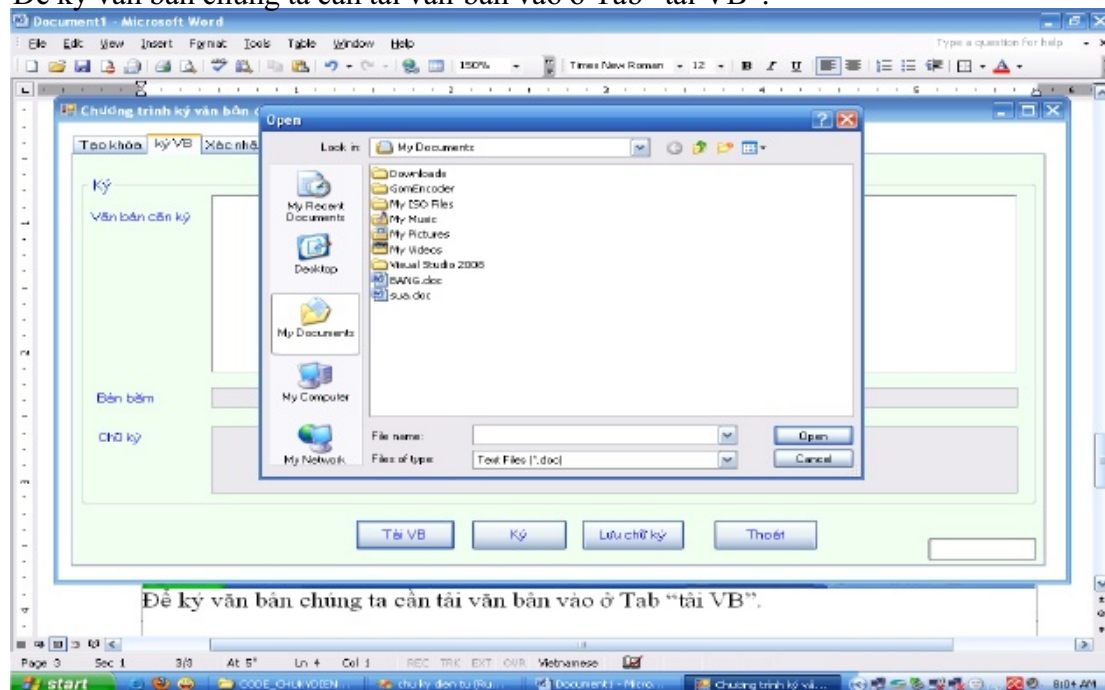
Trước tiên phải chọn các số nguyên tố đủ lớn để khóa khó có thể bẻ gãy (chọn càng lớn thì ký (mã hóa) càng lâu). Sau đó nhấn chọn tính để tại ra cặp khóa công khai và bí mật (là cặp số nguyên tương đối lớn).



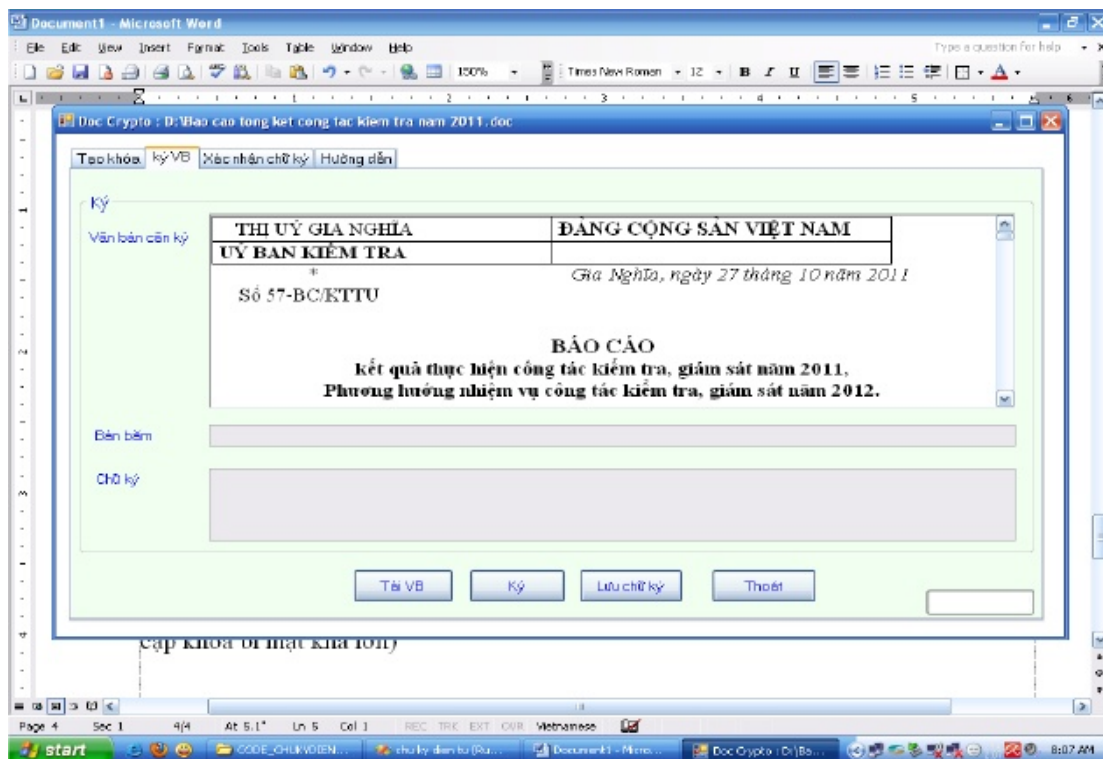
### 3. Ký



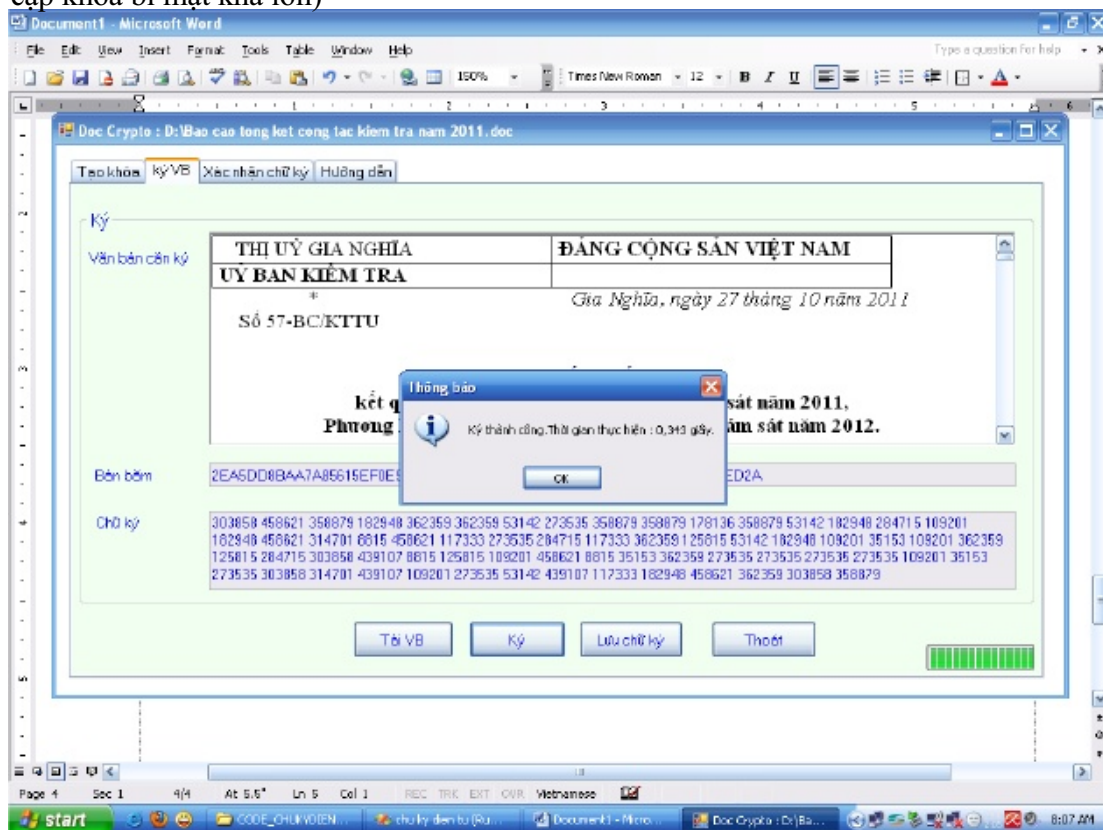
Để ký văn bản chúng ta cần tải văn bản vào ở Tab “tải VB”.



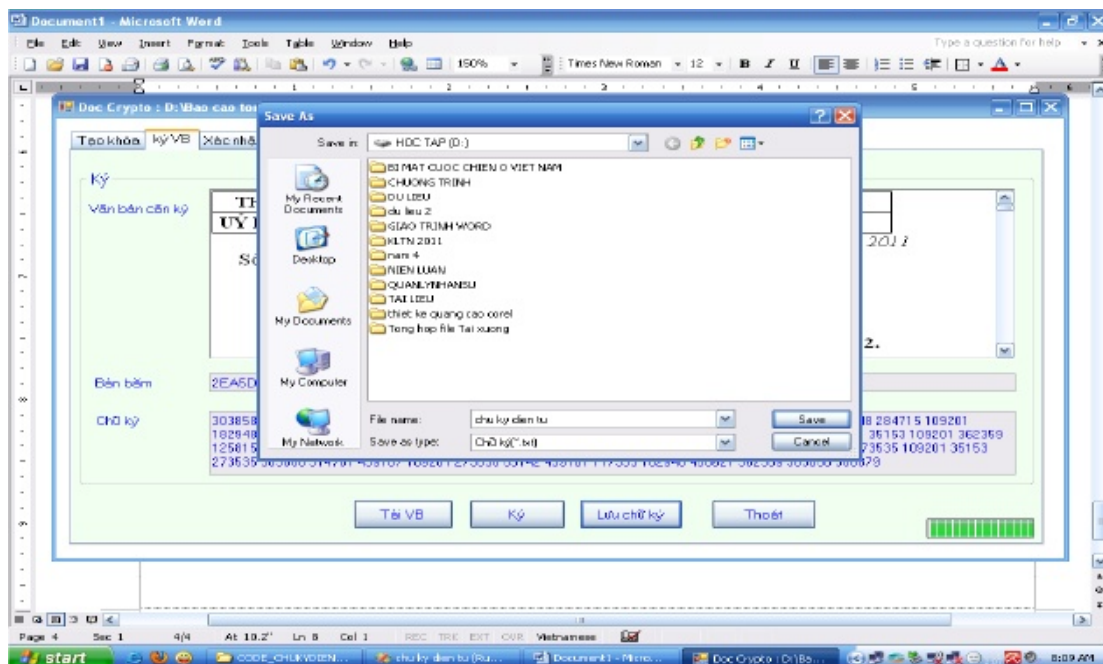
Chọn văn bản cần ký.



Nhấn tab Ký và đợi ct thực hiện bấm văn bản và ký (quá trình ký lâu nếu chúng ta tạo cặp khóa bí mật khá lớn)



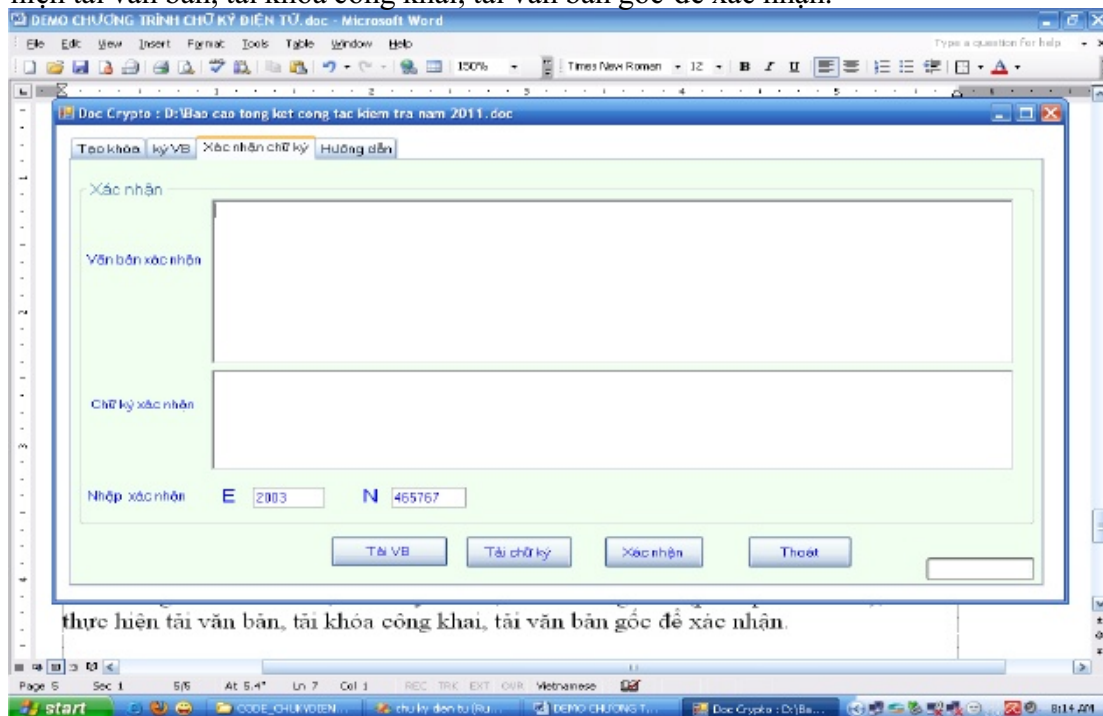
Sau khi ký, chúng ta có bản bìa (SHA or MD5) và chữ ký, thực hiện lưu chữ ký và gửi chữ ký cho người cần xác nhận.



Sau khi ký xong, chúng ta gửi cho người cần xác nhận gồm: Chữ ký, văn bản gốc, và khóa công khai (có thể biết trước từ đầu do cấp phát).

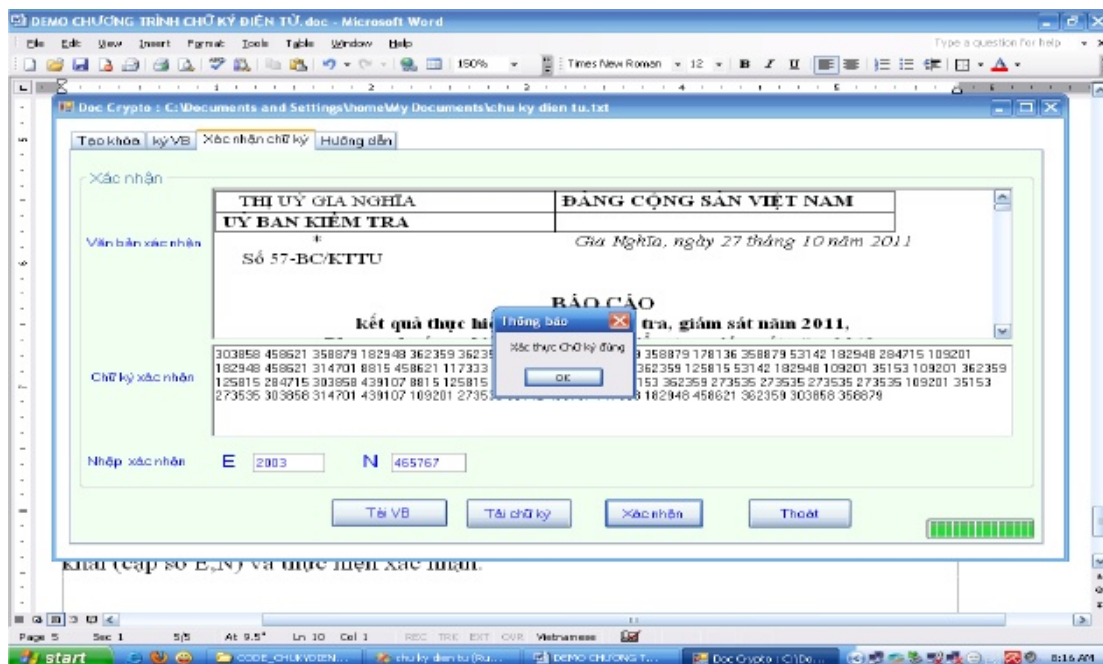
#### 4. xác nhận chữ ký

Sau khi người cần xác nhận chữ ký có được khóa công khai (phân phát từ đầu), sẽ thực hiện tải văn bản, tải khóa công khai, tải văn bản gốc để xác nhận.



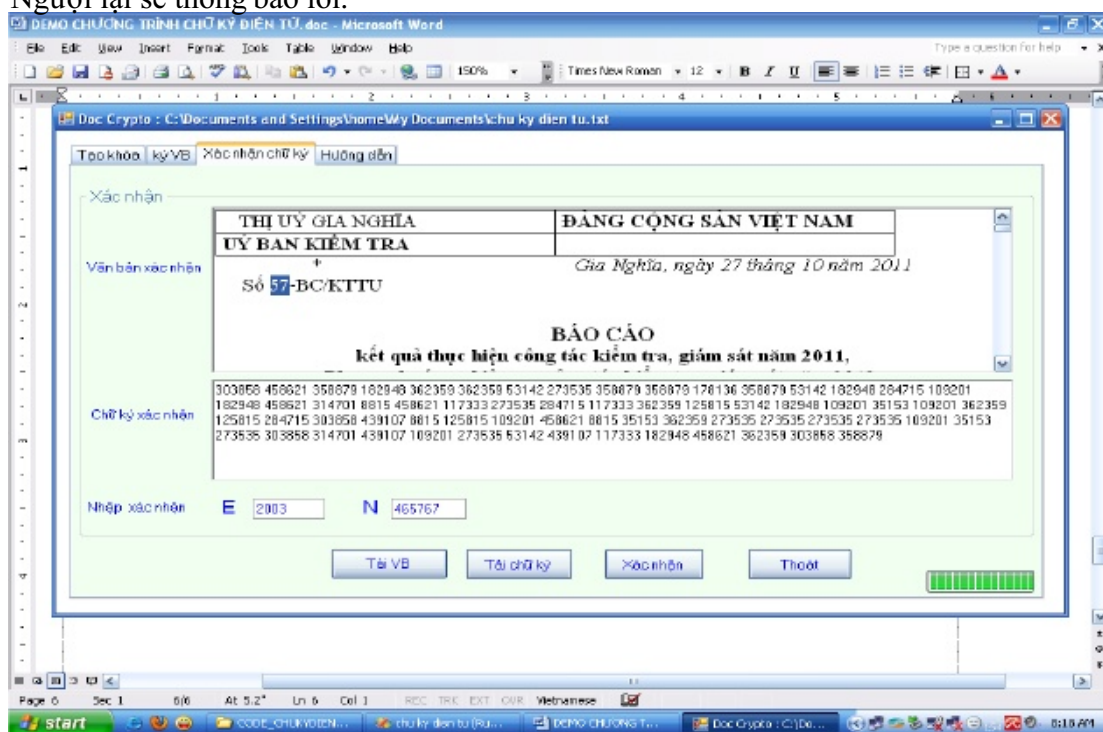
Tải văn bản gốc vào ô văn bản, tải chữ ký vào ô chữ ký xác nhận, nhập khóa công khai (cặp số E,N) và thực hiện xác nhận.

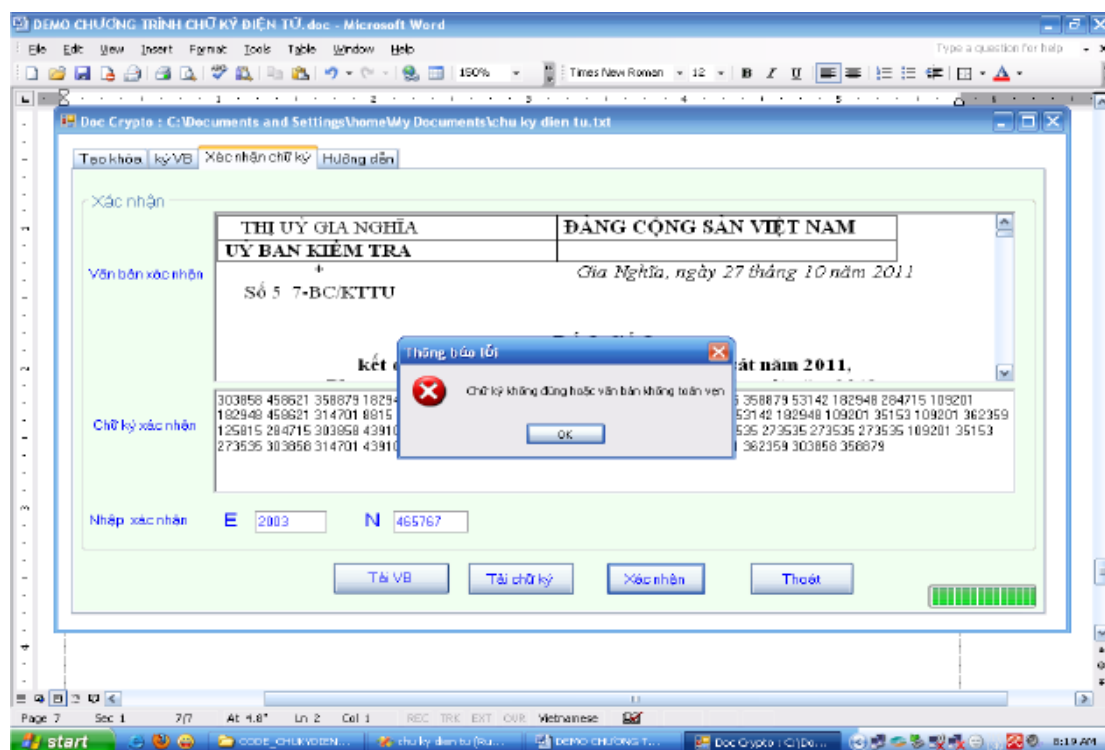
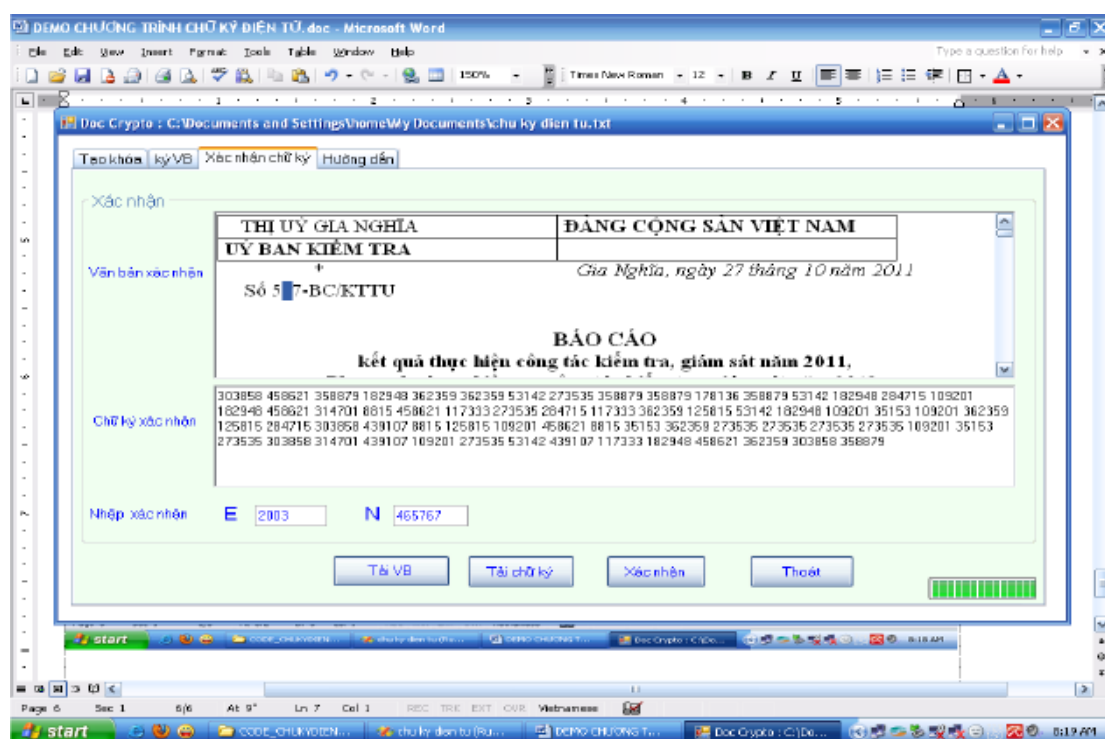




Ct sẽ thông báo chữ ký xác nhận đúng khi: Văn bản gốc không bị sửa đổi (cho dù là một dấu chấm, dấu phẩy, viết hoa hay thường... và chữ ký đúng người ký, khóa công khai đúng của người ký.

Ngược lại sẽ thông báo lỗi.





Mọi thắc mắc và cần **hướng dẫn viết code** xin liên hệ mail: [hainhat007@gmail.com](mailto:hainhat007@gmail.com) để được giải đáp. Lưu ý, các hàm sử dụng trong ct là code theo thuật toán RSA, không sử dụng hàm có sẵn trong thư viện.

