

BAB IV

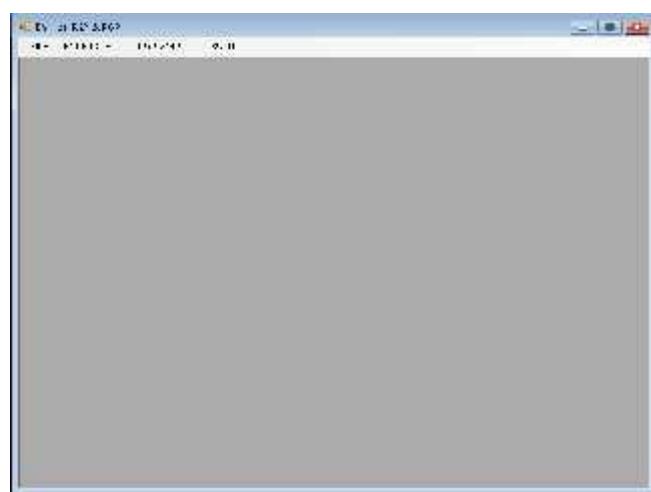
HASIL DAN UJI COBA

IV.1. Uji Coba

Aplikasi RSA dan PGP ini dirancangan untuk berjalan dalam sistem operasi *Windows*. Untuk menjalankan aplikasi ini dapat dilakukan dengan menggunakan aplikasi pembangunnya, yaitu melalui Aplikasi *Visual Studio 2008*, adapun langkah-langkahnya adalah sebagai berikut :

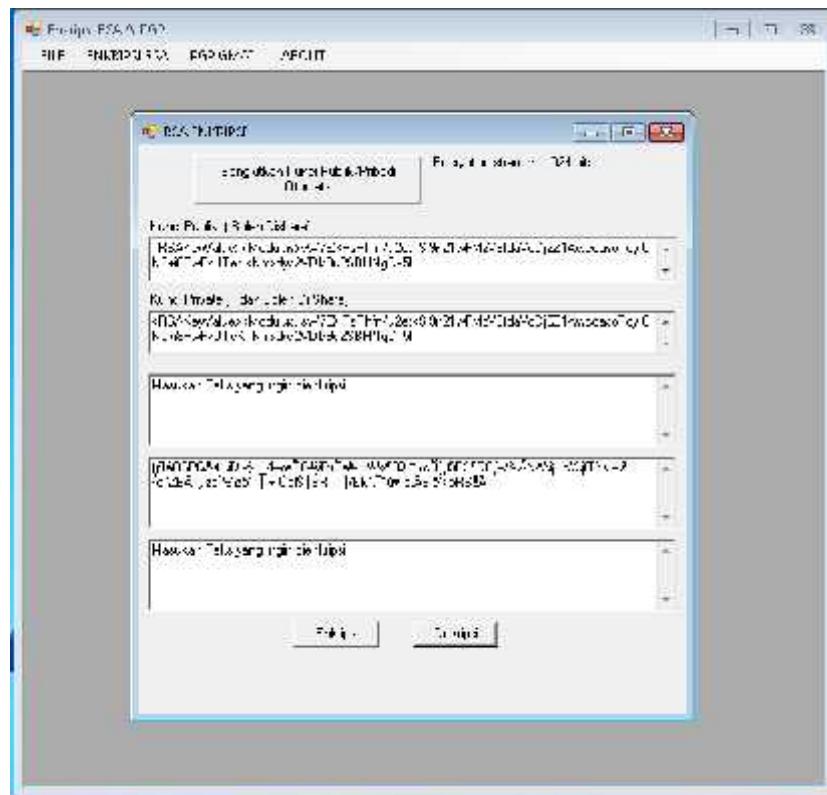
- a. Membuka aplikasi *Visual Studio 2008*.
- b. Pada menu *file* dari aplikasi pilih *Open Project*.
- c. *Browse file vb project* atau *file Microsoft Visual Studio Solution*.
- d. Maka aplikasi ditampilkan dalam *workspace* *Visual Studio 2008*.
- e. Aplikasi dijalankan dengan meng-klik pada *icon Start Debugging* yang terletak pada *toolbar*.

IV.2. Tampilan layar



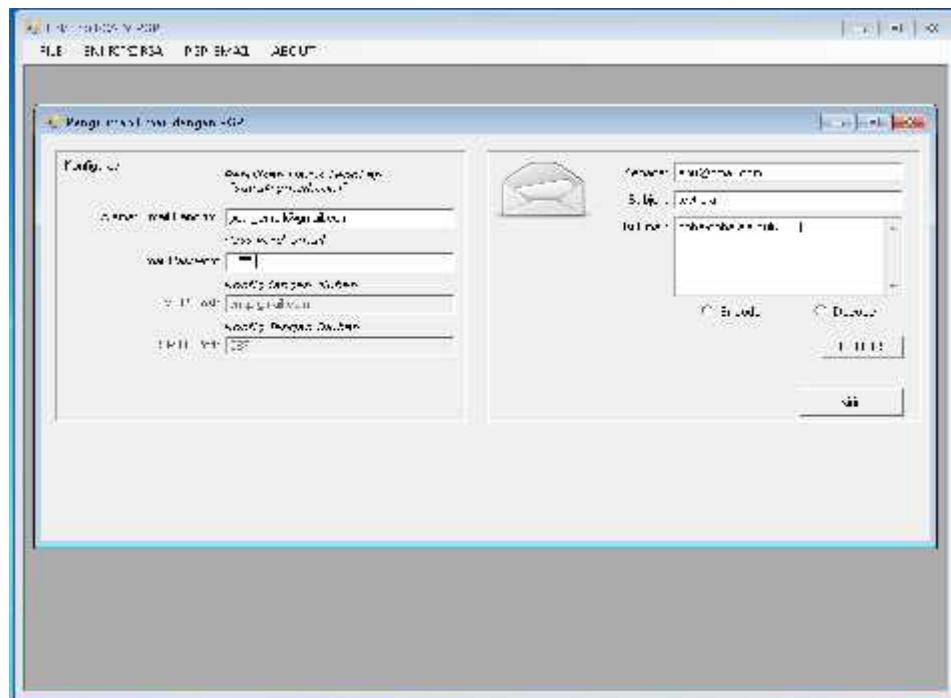
Gambar IV.1. Tampilan hasil dari *form* utama

Tampilan *form* diatas merupakan tampilan *form* yang pertama sekali muncul saat aplikasi dijalankan. Didalam *form* tersebut terdapat empat buah menu yaitu *File*, Enkripsi RSA, PGP Gmail dan About. Masing-masing menu akan terhubung ke *form-form* selanjutnya.

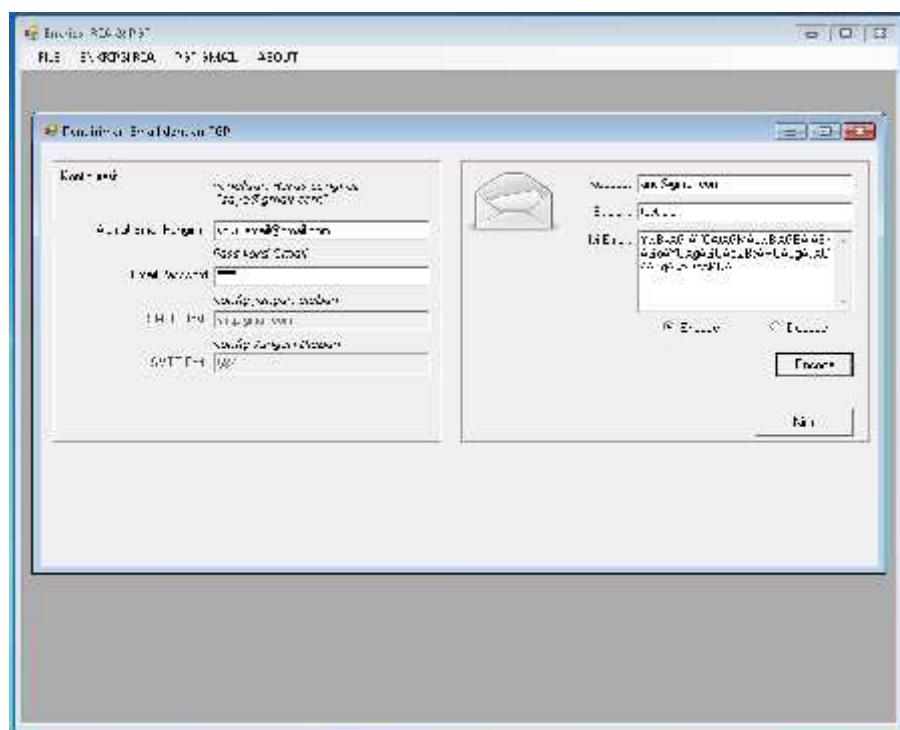


Gambar IV.2. Tampilan *form* menu Enkripsi RSA

Gambar IV.2. adalah tampilan dari *form* enkripsi RSA, dimana pada tampilan gambar terlihat bahwa proses enkripsi telah berhasil dilakukan.



Gambar IV.3. Tampilan Form Pengiriman Email Dengan PGP (Sebelum Enkripsi)



Gambar IV.4. Tampilan Form Pengiriman Email Dengan PGP (Setelah Dekripsi)

Gambar IV.3 dan IV.4 adalah merupakan tampilan hasil dari *form pengiriman email* dengan PGP yang menampilkan kondisi sebelum dan sesudah *file* dienkripsi sebelum dilakukan proses pengiriman.

IV.3. Hardware/Software yang dibutuhkan

Untuk menjalankan aplikasi ini tidak dibutuhkan perangkat dengan *spesifikasi* yang tinggi, berikut adalah kebutuhan *spesifikasi* minimal untuk menjalankan aplikasi ini :

1. Perangkat Keras (*hardware*) yang dibutuhkan :
 - a. Minimal *prosessor Intel Pentium IV 2,4 Ghz*
 - b. Memori 1 Gb.
 - c. Minimal ruang *hard disk* 100 Mb
 - d. Monitor *Standar SVGA*
 - e. *Mouse* dan *keyboard Standard*
2. Perangkat lunak (*software*) yang dibutuhkan :
 - a. Operasi Sistem *Windows XP / Windows 7*
 - b. *.Net Framework 3.5*
 - c. *Microsoft Visual Studio 2008*

IV.4. Analisa hasil

Berdasarkan hasil seluruh rangkaian proses yang telah dilakukan, maka dapat dihasilkanlah analisa sebagai berikut :

1. Untuk melakukan proses enkripsi dan dekripsi dengan menggunakan algoritma RSA dibutuhkan dua buah kunci, yaitu kunci publik dan kunci pribadi.
2. Karakter dari kunci pribadi memiliki jumlah yang jauh lebih besar dibandingkan jumlah karakter yang dimiliki oleh kunci publik.
3. Dengan adanya Kunci publik dan kunci pribadi maka enkripsi yang dihasilkan akun sulit untuk diketahui oleh pihak lain.
4. RSA menghasilkan *byte array* sebesar 1024 *byte*.
5. Proses enkripsi untuk pesan dengan jumlah karakter yang panjang akan membutuhkan waktu yang lebih lama.
6. Proses dekripsi dari pesan membutuhkan waktu yang lebih lama dibandingkan dengan proses enkripsi.
7. Kriptografi dapat diterapkan didalam proses pengiriman *email*, sehingga keamanan dari email yang dikirimkan dapat terjaga dengan baik.

TABEL IV.1. Tabel Pengujian Algoritma RSA

NO	Kunci Publik	Kunci Private	Teks Asli	Enkripsi
1	<RSAKeyValue><Modulus>xVfim6Uq13B EAnRlvR/9Ak3nLoT4lvZMFDF20RUnDC Z17Ca08X7HsU7LlxyIQ3L3Phs6VJ2rJUzc LrtXHlxOooRJ1ZVyu/AYdCtZ/VYeaEuXY VSS/AsLauJSNV3YKtEhq5RQidfOb2edbr3 vP1/AVXAA6NWr3keWCRA+t/HPr0c=</ Modulus><Exponent>AQAB</Exponent>< P>65FkcGEcNG8LnPlMtT4seaHex6Fzbhk XaPgNgr9uCa9EN0xjVarIYwqH5oz/7nSrE kgEDXWR2ZZPdz2mwhqSiw==</P><Q>1 nW+ZPKoOgPTfSc4aY8d705KLgxNgj+C YG/F9dOf0pQXKPYbm1pCojWCZ1AeEn T1qiqpP9eC36JYVVY633XOZtQ==</Q><D P>ubpFPVFjYnfW6SmpcBCYEkIsmqrRjo T+fxVr2ZVClcIo/4xrmURwf53y7jRnKMO 1iVFcWJxEpRAckT/7dXhr5w==</DP><D Q>m/JyyKVLfyRZHaDvfJL9iY68kk+P7S6 Rd97PbLq+dToKvVZ5LLatzZZrhQTVWU aDfYIYILxuBoDfCxgEy5vMIQ==</DQ><I nverseQ>6pRlpYk0Omp8FY7qcTsaTrMwej OHtiLbiuT5frYPD4otLdsCcro0EBIicYgV+e WwegCgV59PwhD72vGLRzTsiA==</Inver seQ><D>ospCxr5TPvD/ST8XhhHTNolpA XjzUCTQ0X+UUhmu4lj/wdSUQvqgZGVp kLgat/kod3UigxalTdm/cFVeIk9nFTnqp2X Qpb+vBe71h3OqWIrWAqxVUJJczvxMrID iqGZe1a57Pwbubv6tp+LDMf/4AYx08ismd gIYidmHhKNUI3E=</D></RSAKeyValue>	STMIK POTENSI UTAMA	O Ó,,\$ö — ·IÓ/4<£{,·í(é5Z ©ò×©ÿ”í³ld5³* ãD— #j=ñÜälR@.... \é<5=KyÓAU ^p Ä“>n*,öÅ' .qóćóy»e&...û o-I,áý)oœÅó× Dz9bÖP\$¶áy* % V&ÙâÅ•P PÀý	
2	<RSAKeyValue><Modulus>tY+qf4kfm2 WS88SANR8fa+LZ5iufugbXlql1oazM2r6 CRyBrs188Y/z/mLkOcDWiqG5N1k/5TIs 7di0HMscYtjSINLAapj8EIzng/yNopswnh	<RSAKeyValue><Modulus>tY+qf4kfm2W S88SANR8fa+LZ5iufugbXlql1oazM2r6CR yBrs188Y/z/mLkOcDWiqG5N1k/5TIs7di0 HMscYtjSINLAapj8EIzng/yNopswnh9bdv	YOS SUDARSO	^m·lòGÙ€uO }ÃÉÄxÖ9"iŠ- d'TcÌD¢ÝÃ§Ü ÄÆ

	9bdvxAQiJNdE8ft8wy7jBFUflJSbTgkC9GDIZ/V5B5zm3hPNxew6rBY0X/4h80=</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>	xAQiJNdE8ft8wy7jBFUflJSbTgkC9GDIZ/V5B5zm3hPNxew6rBY0X/4h80=</Modulus><Exponent>AQAB</Exponent><P>/2Z0z Eev7pPjaiPVpxt/w9/qVntHIEK5mmnzPwG quelDLjAN1Vo96phNt/WPK77Pv4pAhIzj mtrQEn6vQZypXw==</P><Q>tfzRjdEN7n 5iOfW3b7CWMCNE9GmHKZMA2rQ78a Oytox8frO5kFZZ9xJW3qItsIOJMNXn0I3T C0F3MfwT7EiUw==</Q><DP>AkOhQ3J bP+01teotabbXsh/ZDv02zDyvMow/6M4V+ mH0A4PPi5WqONsyzS+zHjsplPicIpjNis8 bv2KhjViVw==</DP><DQ>EXSUbPPWU D/TEBgfZhkb7rYTURYmHri45kFPVpgK9 jN3ZXe7nrqJmocpyeToWPvk1shNmdVgnr 3CvwqfFfu5fQ==</DQ><InverseQ>i4nunN 0j2TuK9VBfX1Nfi3GaRIYqKoHbuPRSJ8a j1vSvdg7IKOsVw8tqcdrrpXQdUmYMEOD VS39z0Iyg/cKhyA==</InverseQ><D>MZs pKGNCwWaFOhksNldkjGOUyXCN2ZPY/ 48ZVq0R44o9qhVPl9ijdWZAp4eYTEw7Pu 20UqPTJ3i7LFStLM62akqCwx20w7tPDA3 KSnzroh+L/q1vvKma64oUAPzclhP2dhvTO Ad7SACyduQAQK22+EYEHmbOB3IA/I2S PUOgXnk=</D></RSAKeyValue>	l- ^{ã/JC†°} l- ^{^aÖ^aÅ•pš¼} Ýó^ Cy3{P ö';0J+ tç<w“úoÑuìà_ Í*†ÚIÝUaûº=7 K - ½ ^{- Ó/QLnxñ} >€IÜž
3	<RSAKeyValue><Modulus>oOWMREFC17Ck3X4Rv1M+d+yli/VlciAN/17dc2t/iGDh8LN/y87Iej88x/0SHdoAH+HsJ8QTEQPkC+Lg68y5VYiejsQfHgNfAvIhuaQiwogLKgxe3Oa3hQ/c/h5vyFJkKPbsdZZCf3XBtRm/R92fPeyr1b8C113yCESIWrxT8uk=</Modulus><Exponent>AQAB</Exponent><P>4QT1V/K2yFgfSWd00pj+G0Awsq+vsf+4+podELNdIA6FK0uemsbu3+x3OCa2/h5d3G77368ynjctmN3rDpx/qQ==</P><Q>twyRumxA	MAHASISWA	{ ¡ÂAušl §ê, Ü ÉÊ ^a · M@ž á Éml RGa!?yXrÁY ÂïèI TM Ý2B <hr/> ÃeË TM Ãèfýÿ Ü2Úf�R ð¾

	ZgsjFPjFkNNArP948hF8Rwnhr6FuYP8NK M61ayfyTVdChko9CCmTiPIP ygEJLnCX0i YmXDm9cThQQ==</Q><DP>r4WzJDxW qcZbeVWzAceHh1g15Fw4r58q+ogWnf1bx G7jH9eXu2Hr2U3J3UoNugGT86u620v9Lv 8ZmUGZ5kbbKQ==</DP><DQ>KVCK87b M6c82/tVQRA4cq6eEfo0NfEYmhbsq45xu qFLPTLsRtZBd15GmNLPJ1YkuAVM+3Cs xO+Be0QMynfY6AQ==</DQ><InverseQ> y9Mj9ai5/Imm0ZQRvHdiBwy5lO5ZfQ9W +MWpIiICFKnYbisxSInkC6ciB9QxQqLdu Lok6fMllJnGTwTvHTMdQ==</InverseQ> <D>ecwq+YRZoEOVGiKUNrxCXrAixac3 a0Q+tGFQzE3FFi0Y/Ig1JshbVMdIMLAvp a9gRsJUbens8QV7/U97KqUoahWACT7Cj CCC4lS6YCNPfZgu255t9AVm7hQAt84yh eLwzqnZfGsvX1fZQhJdo5D04tGgrwZ59Td DZya6rPdqxgE=</D></RSAKeyValue>	ç‰ PbŒÍ³/ ¤ÅòÂ çö— £*ÄK]"äB³R b¶ 9µ□p÷K ÀÂÚ?hv- S"2¢*óf(
4	<RSAKeyValue><Modulus>3z55nk9coJb e5uzKalREzlPqvg6VM4GJdm1I4BdI4DY aFHZj5n/hUxkXuOmUljpIJpkkZO9drDyy qsqkp2VleYtYgUMgf+OJCUq99u8dK62 UxUIYH52x4oa0mlYmXp2vS5BINCbkpr 5p8rNojpubyuBiebOTyVgCTzCMtyeXly8 =</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>	<p>TEKNIK INFORMATIKA</p> <p>\©Ö:- bW¼`© Néê &ùå!P=“à·ÄIÈè àkî,,@öK\$PÝ KŠ: hjkŽ@)š j n¤ ð±'ûÐ*’N € -Fi:\éd- ÎÙ©êÆ“ - yùÉ¢*úÓ¤ë ~Öéµ!...=D4; Ôk□h>u¶;ÉjW ÄÄä«</p>

		KeK+saKm3KXqoowrAq05Q3tCmtxU86z1dCFX5ExgYegPddM+uj+tz3weHc803FeZGtjQQwyEQ0bgQ1rsQ==</DQ><InverseQ>3eFn0jv/cBSA6+9CtNajIf7Ah1zDvm4+s/mN+QNLGpbztWq+rQmfelgCohoaOyGmsy5skiOQ4rBr7nkoEr7amw==</InverseQ><D>a9e3UpWN7nnTZgSfZ6wbrPx22qcaxk3eRNpYKQC2kLEx+g6TBedixwzJG+eigsvWzOaP4T6MpsaPnNfVoJPn518VFxW0Po8LnkQPAFJf1BKqBUZUepEXs/wclzNAuSW9Dh+Wg30UIf49RiNiE03FZ3FIfg2z1EPaotuW97JQIk=</D></RSAKeyValue>		
5		<RSAKeyValue><Modulus>mzYqw50uUzXr6MQZvEP3j6j6MvKIoW76zScC821qxCCYBERp6x1vp4inWXbcBUhd4vt7EZFdZodZXmqGuuJaoOqN6ZKlfn81XTdWNen3+LWb+DN852VESLqt4tv2Ob1g38JFCL3m066DlqXCcRCT2xpvcGb+AQy6FoaYzXCcHS1BE=</Modulus><Exponent>AQAB</Exponent><P>04+7LzKONeoGqX1hILq0dNlaiCZBAbYATaSW2aNa67pv/o1rxgTJifjO98/n2GjnGfo89CKGgNj2TR+EqLw3rQ==</P><Q>u9BXbSbVUwwOTpct/1BZmEGRkO/LveZ6cVQnErZBOKiOsgA3YDclDeszTlrwwwkWpL0+2ZiCPUjPQDj8jrcqdQ==</Q><DP>Tgo0A0oD2XF1ea0NXRRiIsRWt+hcjHZrYbi4CJpQnKoS/kA62+ypFmKhzFDFbpEnXmIaIof0YG3AWYB+nhL1Q==</DP><DQ>sQhmkFWteVWA2uW4DtRfT5xmqPbP1tW8jryjBAIVmyGPOAvqJsB0JhWQzAf+r+kONgTIjHUsNrY93SyaK7BNzQ==</DQ><InverseQ>KdsVLeYW4Nthdbz8kbKxkg+YxPtUtHf7GOOxZXC/4IJ93Ze6j66u2qCjZvLmI/Ob+zor6g9ma2TppXvrgSmPTg==</InverseQ>	SARJANA	8§v1,ºOC[}JQ ...ýiÝ÷¤fÝÒ© žýj3BDÓ4š»cp œþ<þ««f8i½c E7^3^O§wf - Á-tÔš([Çmj]2önö O6.0—]ÆíÉ·`õ(qæý V9Æ³Rü5íýAw W°cIU“èIëŒ ...<i‡Æå?Ø

	/InverseQ><D>bjMYS8jWskfPlnVdHFlZd Mtx0Sh4L74/Hde79Z/TNSs7I5R7a2577wR MZw3Jq4qE9nq9F20ZMJtcqGnDvIQwYU QTcjE9eAXpi+LBNDzKN3SVLmO51y2bl CikFsVY5QthK+CbvfSbZhVz6u6OISuhbX yqxooEAQUDK6DZWhxedE=</D></RSA KeyValue>		
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

IV.5. Kelebihan dan kekurangan

Berikut adalah merupakan sisi kelebihan dari aplikasi RSA dan PGP yang telah penulis rancang :

1. Tidak membutuhkan spesifikasi perangkat yang tinggi untuk menjalankan aplikasi.
2. Memiliki tampilan yang sederhana, sehingga mudah dimengerti.
3. Pada Enkripsi RSA proses pembuatan kunci publik dan pribadi dilakukan secara otomatis.
4. Hasil dari enkripsi yang telah dihasilkan tidak bisa didekripsi oleh aplikasi lain
5. Pada PGP *host smtp* dan *port smtp* telah diatur dalam aplikasi, sehingga pengguna tidak merlu melakukan konfigurasi ulang.

Sementara kekurangan yang dimiliki oleh aplikasi ini adalah :

1. Tampilan dari aplikasi sedehana dan hanya menggunakan tampilan *default* dari aplikasi yang membangunnya.
2. Hasil dari proses enkripsi tidak bisa disimpan kedalam bentuk *file*.
3. Pada enkripsi RSA tidak didesain untuk melakukan enkripsi terhadap data yang sudah berbentuk *file*.
4. Untuk PGP hanya menggunakan *port smtp gmail*, sehingga pengirim tidak dapat melakukan pengiriman dengan menggunakan alamat *email dari mail server* lainnya.
5. Aplikasi PGP yang dihasilkan belum bisa berfungsi untuk menerima pesan yang dikirimkan oleh pihak lain.