and the presence of nulls. In short, they were able to break the majority of encrypted messages. Their skills provided a steady flow of uncovered secrets, which influenced the decisions of their masters and mistresses, thereby affecting Europe's history at critical moments.

Nowhere is the impact of cryptanalysis more dramatically illustrated than in the case of Mary Queen of Scots. The outcome of her trial depended wholly on the battle between her codemakers and Queen Elizabeth's codebreakers. Mary was one of the most significant figures of the sixteenth century–Queen of Scotland, Queen of France, pretender to the English throne–yet her fate would be decided by a slip of paper, the message it bore, and whether or not that message could be deciphered.

The Babington Plot

On November 24, 1542, the English forces of Henry VIII demolished the Scottish army at the Battle of Solway Moss. It appeared that Henry was on the verge of conquering Scotland and stealing the crown of King James V. After the battle, the distraught Scottish king suffered a complete mental and physical breakdown, and withdrew to the palace at Falkland. Even the birth of a daughter, Mary, just two weeks later could not revive the ailing king. It was as if he had been waiting for news of an heir so that he could die in peace, safe in the knowledge that he had done his duty. Just a week after Mary's birth, King James V, still only thirty years old, died. The baby princess had become Mary Queen of Scots.

Mary was born prematurely, and initially there was considerable concern that she would not survive. Rumors in England suggested that the baby had died, but this was merely wishful thinking at the English court, which was keen to hear any news that might destabilize Scotland. In fact, Mary soon grew strong and healthy, and at the age of nine months, on September 9, 1543, she was crowned in the chapel of Stirling Castle, surrounded by three earls, bearing on her behalf the royal crown, scepter and sword.

The fact that Queen Mary was so young offered Scotland a respite from English incursions. It would have been deemed unchivalrous had Henry VIII attempted to invade the country of a recently dead king, now under the rule of an infant queen. Instead, the English king decided on a policy of

wooing Mary in the hope of arranging a marriage between her and his son Edward, thereby uniting the two nations under a Tudor sovereign. He began his maneuvering by releasing the Scottish nobles captured at Solway Moss, on the condition that they campaign in favor of a union with England.

However, after considering Henry's offer, the Scottish court rejected it in favor of a marriage to Francis, the dauphin of France. Scotland was choosing to ally itself with a fellow Roman Catholic nation, a decision which pleased Mary's mother, Mary of Guise, whose own marriage with James V had been intended to cement the relationship between Scotland and France. Mary and Francis were still children, but the plan for the future was that they would eventually marry, and Francis would ascend the throne of France with Mary as his queen, thereby uniting Scotland and France. In the meantime, France would defend Scotland against any English onslaught.

The promise of protection was reassuring, particularly as Henry VIII had switched from diplomacy to intimidation in order to persuade the Scots that his own son was a more worthy groom for Mary Queen of Scots. His forces committed acts of piracy, destroyed crops, burned villages and attacked towns and cities along the border. The "rough wooing," as it is known, continued even after Henry's death in 1547. Under the auspices of his son, King Edward VI (the would-be suitor), the attacks culminated in the Battle of Pinkie Cleugh, in which the Scottish army was routed. As a result of this slaughter it was decided that, for her own safety, Mary should leave for France, beyond the reach of the English threat, where she could prepare for her marriage to Francis. On August 7, 1548, at the age of six, she set sail for the port of Roscoff.

Mary's first few years in the French court would be the most idyllic time of her life. She was surrounded by luxury, protected from harm, and she grew to love her future husband, the dauphin. At the age of sixteen they married, and the following year Francis and Mary became King and Queen of France. Everything seemed set for her triumphant return to Scotland, until her husband, who had always suffered from poor health, fell gravely ill. An ear infection that he had nursed since a child had worsened, the inflammation spread toward his brain, and an abscess began to develop. In 1560, within a year of being crowned, Francis was dead and Mary was widowed.

From this point onward, Mary's life would be repeatedly struck by tragedy. She returned to Scotland in 1561, where she discovered a transformed nation. During her long absence Mary had confirmed her Catholic faith, while her Scottish subjects had increasingly moved toward the Protestant church. Mary tolerated the wishes of the majority and at first reigned with relative success, but in 1565 she married her cousin, Henry Stewart, the Earl of Darnley, an act that led to a spiral of decline. Darnley was a vicious and brutal man whose ruthless greed for power lost Mary the loyalty of the Scottish nobles. The following year Mary witnessed for herself the full horror of her husband's barbaric nature when he murdered David Riccio, her secretary, in front of her. It became clear to everyone that for the sake of Scotland it was necessary to get rid of Darnley. Historians debate whether it was Mary or the Scottish nobles who instigated the plot, but on the night of February 9, 1567, Darnley's house was blown up and, as he attempted to escape, he was strangled. The only good to come from the marriage was a son and heir, James.

Mary's next marriage, to James Hepburn, the Fourth Earl of Bothwell, was hardly more successful. By the summer of 1567 the Protestant Scottish nobles had become completely disillusioned with their Catholic Queen, and they exiled Bothwell and imprisoned Mary, forcing her to abdicate in favor of her fourteen-month-old son, James VI, while her half-brother, the Earl of Moray, acted as regent. The next year, Mary escaped from her prison, gathered an army of six thousand royalists, and made a final attempt to regain her crown. Her soldiers confronted the regent's army at the small village of Langside, near Glasgow, and Mary witnessed the battle from a nearby hilltop. Although her troops were greater in number, they lacked discipline, and Mary watched as they were torn apart. When defeat was inevitable, she fled. Ideally she would have headed east to the coast, and then on to France, but this would have meant crossing territory loyal to her half-brother, and so instead she headed south to England, where she hoped that her cousin Queen Elizabeth I would provide refuge.

Mary had made a terrible misjudgment. Elizabeth offered Mary nothing more than another prison. The official reason for her arrest was in connection with the murder of Darnley, but the true reason was that Mary posed a threat to Elizabeth, because English Catholics considered

Mary to be the true queen of England. Through her grandmother, Margaret Tudor, the elder sister of Henry VIII, Mary did indeed have a claim to the throne, but Henry's last surviving offspring, Elizabeth I, would seem to have a prior claim. However, according to Catholics, Elizabeth was illegitimate because she was the daughter of Anne Boleyn, Henry's second wife after he had divorced Catherine of Aragon in defiance of the Pope. English Catholics did not recognize Henry VIII's divorce, they did not acknowledge his ensuing marriage to Anne Boleyn, and they certainly did not accept their daughter Elizabeth as Queen. Catholics saw Elizabeth as a bastard usurper.

Mary was imprisoned in a series of castles and manors. Although Elizabeth thought of her as one of the most dangerous figures in England, many Englishmen admitted that they admired her gracious manner, her obvious intelligence and her great beauty. William Cecil, Elizabeth's Great Minister, commented on "her cunning and sugared entertainment of all men," and Nicholas White, Cecil's emissary, made a similar observation: "She hath withal an alluring grace, a pretty Scotch accent, and a searching wit, clouded with mildness." But, as each year passed, her appearance waned, her health deteriorated and she began to lose hope. Her jailer, Sir Amyas Paulet, a Puritan, was immune to her charms, and treated her with increasing harshness.

By 1586, after 18 years of imprisonment, she had lost all her privileges. She was confined to Chartley Hall in Staffordshire, and was no longer allowed to take the waters at Buxton, which had previously helped to alleviate her frequent illnesses. On her last visit to Buxton she used a diamond to inscribe a message on a windowpane: "Buxton, whose warm waters have made thy name famous, perchance I shall visit thee no more–Farewell." It appears that she suspected that she was about to lose what little freedom she had. Mary's growing sorrow was compounded by the actions of her nineteen-year-old son, King James VI of Scotland. She had always hoped that one day she would escape and return to Scotland to share power with her son, whom she had not seen since he was one year old. However, James felt no such affection for his mother. He had been brought up by Mary's enemies, who had taught James that his mother had murdered his father in order to marry her lover. James despised her, and feared that if she returned then she might seize his crown. His hatred

toward Mary was demonstrated by the fact that he had no qualms in seeking a marriage with Elizabeth I, the woman responsible for his mother's imprisonment (and who was also thirty years his senior). Elizabeth declined the offer.

Mary wrote to her son in an attempt to win him over, but her letters never reached the Scottish border. By this stage, Mary was more isolated then ever before: all her outgoing letters were confiscated, and any incoming correspondence was kept by her jailer. Mary's morale was at its lowest, and it seemed that all hope was lost. It was under these severe and desperate circumstances that, on January 6, 1586, she received an astonishing package of letters.

The letters were from Mary's supporters on the Continent, and they had been smuggled into her prison by Gilbert Gifford, a Catholic who had left England in 1577 and trained as a priest at the English College in Rome. Upon returning to England in 1585, apparently keen to serve Mary, he immediately approached the French Embassy in London, where a pile of correspondence had accumulated. The Embassy had known that if they forwarded the letters by the formal route, Mary would never see them. However Gifford claimed that he could smuggle the letters into Chartley Hall, and sure enough he lived up to his word. This delivery was the first of many, and Gifford began a career as a courier, not only passing messages to Mary but also collecting her replies. He had a rather cunning way of sneaking letters into Chartley Hall. He took the messages to a local brewer, who wrapped them in a leather packet, which was then hidden inside a hollow bung used to seal a barrel of beer. The brewer would deliver the barrel to Chartley Hall, whereupon one of Mary's servants would open the bung and take the contents to the Queen of Scots. The process worked equally well for getting messages out of Chartley Hall.

Meanwhile, unknown to Mary, a plan to rescue her was being hatched in the taverns of London. At the center of the plot was Anthony Babington, aged just twenty-four but already well known in the city as a handsome, charming and witty bon viveur. What his many admiring contemporaries failed to appreciate was that Babington deeply resented the establishment, which had persecuted him, his family and his faith. The state's anti-Catholic policies had reached new heights of horror, with priests being

accused of treason, and anybody caught harboring them punished by the rack, mutilation and disemboweling while still alive. The Catholic mass was officially banned, and families who remained loyal to the Pope were forced to pay crippling taxes. Babington's animosity was fueled by the death of Lord Darcy, his great-grandfather, who was beheaded for his involvement in the Pilgrimage of Grace, a Catholic uprising against Henry VIII.

The conspiracy began one evening in March 1586, when Babington and six confidants gathered in The Plough, an inn outside Temple Bar. As the historian Philip Caraman observed, "He drew to himself by the force of his exceptional charm and personality many young Catholic gentlemen of his own standing, gallant, adventurous and daring in defense of the Catholic faith in its day of stress; and ready for any arduous enterprise whatsoever that might advance the common Catholic cause." Over the next few months an ambitious plan emerged to free Mary Queen of Scots, assassinate Queen Elizabeth and incite a rebellion supported by an invasion from abroad.

The conspirators were agreed that the Babington Plot, as it became known, could not proceed without the blessing of Mary, but there was no apparent way to communicate with her. Then, on July 6, 1586, Gifford arrived on Babington's doorstep. He delivered a letter from Mary, explaining that she had heard about Babington via her supporters in Paris, and looked forward to hearing from him. In reply, Babington compiled a detailed letter in which he outlined his scheme, including a reference to the excommunication of Elizabeth by Pope Pius V in 1570, which he believed legitimized her assassination.

> Myself with ten gentlemen and a hundred of our followers will undertake the delivery of your royal person from the hands of your enemies. For the dispatch of the usurper, from the obedience of whom we are by the excommunication of her made free, there be six noble gentlemen, all my private friends, who for the zeal they bear to the Catholic cause and your Majesty's service will undertake that tragical execution.

As before, Gifford used his trick of putting the message in the bung of a beer barrel in order to sneak it past Mary's guards. This can be considered a form of steganography, because the letter was being hidden. As an extra precaution, Babington enciphered his letter so that even if it was

intercepted by Mary's jailer, it would be indecipherable and the plot would not be uncovered. He used a cipher which was not a simple monoalphabetic substitution, but rather a nomenclator, as shown in Figure 8. It consisted of 23 symbols that were to be substituted for the letters of the alphabet (excluding j, v and w), along with 35 symbols representing words or phrases. In addition, there were four nulls (ff.⊢.⊣.d.) and a symbol ơ which signified that the next symbol represents a double letter ("dowbleth").

Gifford was still a youth, even younger than Babington, and yet he conducted his deliveries with confidence and guile. His aliases, such as Mr. Colerdin, Pietro and Cornelys, enabled him to travel the country without suspicion, and his contacts within the Catholic community provided him with a series of safe houses between London and Chartley Hall. However, each time Gifford traveled to or from Chartley Hall, he would make a detour. Although Gifford was apparently acting as an agent for Mary, he was actually a double agent. Back in 1585, before his return to England, Gifford had written to Sir Francis Walsingham, Principal Secretary to Queen Elizabeth, offering his services. Gifford realized that his Catholic background would act as a perfect mask for infiltrating plots

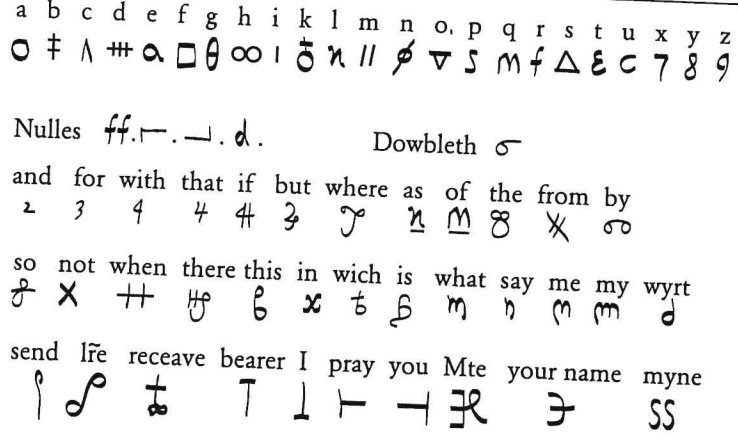

Figure 8 The nomenclator of Mary Queen of Scots, consisting of a cipher alphabet and codewords.

against Queen Elizabeth. In the letter to Walsingham, he wrote, "I have heard of the work you do and I want to serve you. I have no scruples and no fear of danger. Whatever you order me to do I will accomplish."

Walsingham was Elizabeth's most ruthless minister. He was a Machiavellian figure, a spymaster who was responsible for the security of the monarch. He had inherited a small network of spies, which he rapidly expanded into the Continent, where many of the plots against Elizabeth were being hatched. After his death it was discovered that he had been receiving regular reports from twelve locations in France, nine in Germany, four in Italy, four in Spain and three in the Low Countries, as well as having informants in Constantinople, Algiers and Tripoli.

Walsingham recruited Gifford as a spy, and in fact it was Walsingham who ordered Gifford to approach the French Embassy and offer himself as a courier. Each time Gifford collected a message to or from Mary, he would first take it to Walsingham. The vigilant spymaster would then pass it to his counterfeiters, who would break the seal on each letter, make a copy, and then reseal the original letter with an identical stamp before handing it back to Gifford. The apparently untouched letter could then be delivered to Mary or her correspondents, who remained oblivious to what was going on.

When Gifford handed Walsingham a letter from Babington to Mary, the first objective was to decipher it. Walsingham had originally encountered codes and ciphers while reading a book written by the Italian mathematician and cryptographer Girolamo Cardano (who, incidentally, proposed a form of writing for the blind based on touch, a precursor of Braille). Cardano's book aroused Walsingham's interest, but it was a decipherment by the Flemish cryptanalyst Philip van Marnix that really convinced him of the power of having a codebreaker at his disposal. In 1577, Philip of Spain was using ciphers to correspond with his half-brother and fellow Catholic, Don John of Austria, who was in control of much of the Netherlands. Philip's letter described a plan to invade England, but it was intercepted by William of Orange, who passed it to Marnix, his cipher secretary. Marnix deciphered the plan, and William passed the information to Daniel Rogers, an English agent working on the Continent, who in turn warned Walsingham of the invasion. The English reinforced their defenses, which was enough to deter the invasion attempt.

Now fully aware of the value of cryptanalysis, Walsingham established

a cipher school in London and employed Thomas Phelippes as his cipher secretary, a man "of low stature, slender every way, dark yellow haired on the head, and clear yellow bearded, eaten in the face with smallpox, of short sight, thirty years of age by appearance." Phelippes was a linguist who could speak French, Italian, Spanish, Latin and German, and, more importantly, he was one of Europe's finest cryptanalysts.

Upon receiving any message to or from Mary, Phelippes devoured it. He was a master of frequency analysis, and it would be merely a matter of time before he found a solution. He established the frequency of each character, and tentatively proposed values for those that appeared most often. When a particular approach hinted at absurdity, he would backtrack and try alternative substitutions. Gradually he would identify the nulls, the cryptographic red herrings, and put them to one side. Eventually all that remained were the handful of codewords, whose meaning could be guessed from the context.

When Phelippes deciphered Babington's message to Mary, which clearly proposed the assassination of Elizabeth, he immediately forwarded the damning text to his master. At this point Walsingham could have pounced on Babington, but he wanted more than the execution of a handful of rebels. He bided his time in the hope that Mary would reply and authorize the plot, thereby incriminating herself. Walsingham had long wished for the death of Mary Queen of Scots, but he was aware of Elizabeth's reluctance to execute her cousin. However, if he could prove that Mary was endorsing an attempt on the life of Elizabeth, then surely his queen would permit the execution of her Catholic rival. Walsingham's hopes were soon fulfilled.

On July 17, Mary replied to Babington, effectively signing her own death warrant. She explicitly wrote about the "design," showing particular concern that she should be released simultaneously with, or before, Elizabeth's assassination, otherwise news might reach her jailer, who might then murder her. Before reaching Babington, the letter made the usual detour to Phelippes. Having cryptanalyzed the earlier message, he deciphered this one with ease, read its contents, and marked it with a "Π"—the sign of the gallows.

Walsingham had all the evidence he needed to arrest Mary and Babington, but still he was not satisfied. In order to destroy the

conspiracy completely, he needed the names of all those involved. He asked Phelippes to forge a postscript to Mary's letter, which would entice Babington to name names. One of Phelippes's additional talents was as a forger, and it was said that he had the ability "to write any man's hand, if he had once seen it, as if the man himself had writ it." Figure 9 shows the postscript that was added at the end of Mary's letter to Babington. It can be deciphered using Mary's nomenclator, as shown in Figure 8, to reveal the following plaintext:

> I would be glad to know the names and qualities of the six gentlemen which are to accomplish the designment; for it may be that I shall be able, upon knowledge of the parties, to give you some further advice necessary to be followed therein, as also from time to time particularly how you proceed: and as soon as you may, for the same purpose, who be already, and how far everyone is privy hereunto.

The cipher of Mary Queen of Scots clearly demonstrates that a weak encryption can be worse than no encryption at all. Both Mary and Babington wrote explicitly about their intentions because they believed that their communications were secure, whereas if they had been communicating openly they would have referred to their plan in a more discreet manner. Furthermore, their faith in their cipher made them particularly vulnerable to accepting Phelippes's forgery. Sender and receiver often have such confidence in the strength of their cipher that

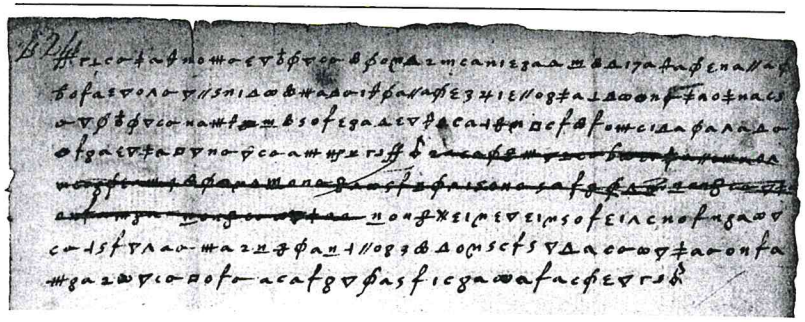

Figure 9 The forged postscript added by Thomas Phelippes to Mary's message. It can be deciphered by referring to Mary's nomenclator (Figure 8).

they consider it impossible for the enemy to mimic the cipher and insert forged text. The correct use of a strong cipher is a clear boon to sender and receiver, but the misuse of a weak cipher can generate a very false sense of security.

Soon after receiving the message and its postscript, Babington needed to go abroad to organize the invasion, and had to register at Walsingham's department in order to acquire a passport. This would have been an ideal time to capture the traitor, but the bureaucrat who was manning the office, John Scudamore, was not expecting the most wanted traitor in England to turn up at his door. Scudamore, with no support to hand, took the unsuspecting Babington to a nearby tavern, stalling for time while his assistant organized a group of soldiers. A short while later a note arrived at the tavern, informing Scudamore that it was time for the arrest. Babington, however, caught sight of it. He casually said that he would pay for the beer and meal and rose to his feet, leaving his sword and coat at the table, implying that he would return in an instant. Instead, he slipped out of the back door and escaped, first to St. John's Wood and then on to Harrow. He attempted to disguise himself, cutting his hair short and staining his skin with walnut juice to mask his aristocratic background. He managed to elude capture for ten days, but by August 15, Babington and his six colleagues were captured and brought to London. Church bells across the city rang out in triumph. Their executions were horrid in the extreme. In the words of the Elizabethan historian William Camden, "they were all cut down, their privities were cut off, bowelled alive and seeing, and quartered."

Meanwhile, on August 11, Mary Queen of Scots and her entourage had been allowed the exceptional privilege of riding in the grounds of Chartley Hall. As Mary crossed the moors she spied some horsemen approaching, and immediately thought that these must be Babington's men coming to rescue her. It soon became clear that these men had come to arrest her, not release her. Mary had been implicated in the Babington Plot, and was charged under the Act of Association, an Act of Parliament passed in 1584 specifically designed to convict anybody involved in a conspiracy against Elizabeth.

The trial was held in Fotheringhay Castle, a bleak, miserable place in the middle of the featureless fens of East Anglia. It began on Wednesday, October 15, in front of two chief justices, four other judges, the Lord

Chancellor, the Lord Treasurer, Walsingham, and various earls, knights and barons. At the back of the courtroom there was space for spectators, such as local villagers and the servants of the commissioners, all eager to see the humiliated Scottish queen beg forgiveness and plead for her life. However, Mary remained dignified and composed throughout the trial. Mary's main defense was to deny any connection with Babington. "Can I be responsible for the criminal projects of a few desperate men," she proclaimed, "which they planned without my knowledge or participation?" Her statement had little impact in the face of the evidence against her.

Mary and Babington had relied on a cipher to keep their plans secret, but they lived during a period when cryptography was being weakened by advances in cryptanalysis. Although their cipher would have been sufficient protection against the prying eyes of an amateur, it stood no chance against an expert in frequency analysis. In the spectators' gallery sat Phelippes, quietly watching the presentation of the evidence that he had conjured from the enciphered letters.

The trial went into a second day, and Mary continued to deny any knowledge of the Babington Plot. When the trial finished, she left the judges to decide her fate, pardoning them in advance for the inevitable decision. Ten days later, the Star Chamber met in Westminster and concluded that Mary had been guilty of "compassing and imagining since June 1st matters tending to the death and destruction of the Queen of England." They recommended the death penalty, and Elizabeth signed the death warrant.

On February 8, 1587, in the Great Hall of Fotheringhay Castle, an audience of three hundred gathered to watch the beheading. Walsingham was determined to minimize Mary's influence as a martyr, and he ordered that the block, Mary's clothing, and everything else relating to the execution be burned in order to avoid the creation of any holy relics. He also planned a lavish funeral procession for his son-in-law, Sir Philip Sidney, to take place the following week. Sidney, a popular and heroic figure, had died fighting Catholics in the Netherlands, and Walsingham believed that a magnificent parade in his honor would dampen sympathy for Mary. However, Mary was equally determined that her final appearance should be a defiant gesture, an opportunity to reaffirm her Catholic faith and inspire her followers.

While the Dean of Peterborough led the prayers, Mary spoke aloud her own prayers for the salvation of the English Catholic Church, for her son and for Elizabeth. With her family motto, "In my end is my beginning," in her mind, she composed herself and approached the block. The executioners requested her forgiveness, and she replied, "I forgive you with all my heart, for now I hope you shall make an end of all my troubles." Richard Wingfield, in his *Narration of the Last Days of the Queen of Scots*, describes her final moments:

> Then she laide herself upon the blocke most quietlie, & stretching out her armes & legges cryed out In manus tuas domine three or foure times, & at the laste while one of the executioners held her slightlie with one of his handes, the other gave two strokes with an axe before he cutt of her head, & yet lefte a little gristle behinde at which time she made verie small noyse & stirred not any parte of herself from the place where she laye . . . Her lipps stirred up & downe almost a quarter of an hower after her head was cutt of. Then one of her executioners plucking of her garters espied her little dogge which was crept under her clothes which could not be gotten forth but with force & afterwardes could not depart from her dead corpse, but came and laye betweene her head & shoulders a thing dilligently noted.

Figure 10 The execution of Mary Queen of Scots.

2 Le Chiffre

For centuries, the simple
sufficient to ensure
frequency analysis, first in
its security. The tragic exec
illustration of the weaknes
battle between cryptograp
cryptanalysts had gained th
message had to accept that
and decipher their most pr

The onus was clearly on
cipher, something that cc
cipher would not emerge u
can be traced back to the
Battista Alberti. Born in 1
the Renaissance—a painter,
author of the first scienti
housefly and a funeral orat
an architect, having desig
written *De re aedificatoria*,
acted as a catalyst for the tr

Sometime in the 1460s,
the Vatican when he bu
pontifical secretary, who b
points of cryptography. T
write an essay on the subjec
of cipher. At the time, all
alphabet for encrypting ea