Careers in Cryptology, codes, code-breaking and encryption
(Developed from AGCAS link enquires, January 2011)

A summary of information received from numerous Careers Services regarding
codes, code-breaking and encryption.

Cryptography is used very widely in:
– mobile phones (protecting calls and texts);
– banking (chip and PIN cards);
– Internet (protecting transaction details using SSL, SSH);
– corporate computer security;
– home computing (Windows and other OSs come with a set of crypto
  algorithms);
– satellite TV (e.g. Sky);

• Data security is a big issue for a number of companies, and banks probably have
  the biggest stake. Internationally, the USA and Australia have massive interest.
• University of Chicago in the USA and Macquarie University in Australia are
  leading universities in the field.
• postgraduate study can be important
• Royal Holloway, University of London runs a MSc in Mathematics of
  Cryptography and Communications (as yet no destination data)
• the International Association for cryptology has a section on jobs & PHD’s in
  cryptology – www.iacr.org/jobs/
• many positions may require Computer Science and/or IT qualifications and
  experience e.g. programming languages
• there may be issues linked to security clearance for some employers (e.g.
  government security services) – international students may need to focus their
  job search on corporate employers

Websites to get started
www.mathscareers.org.uk/viewItem.cfm?cit_id=382816 – an introduction to
cryptography
www.studydiscussions.com/cryptography-as-a-career-option/ - information
(from the US) about cryptography as a career
www.kent.ac.uk/careers/workin/forensiccomputing.htm - an overview of forensic
computing and cryptography careers with lots of useful links.
Potential Employers

- **Government intelligence services** (very limited information available for some services)
  - The Ministry of Defence – jobs available for civilians in the Government Communication Network and positions in the armed forces (although information about specific roles is limited) - [www.mod.uk/DefenceInternet/DefenceFor/Jobseekers/](http://www.mod.uk/DefenceInternet/DefenceFor/Jobseekers/)
  - GCHQ (Government Communications Headquarters) – recruits maths graduates (and related disciplines with significant math content, e.g. statistics, physics or engineering) for mathematical research to help counter threats to British people and interests. Researchers work on some of the world's most challenging cryptographic problems and developing some of the world's most secure systems. - [www.gchq-careers.co.uk/](http://www.gchq-careers.co.uk/)
  - The Communication Electronics Security Group (CESG) is the Information Assurance arm of the Government Communications Headquarters (GCHQ) and it provides advice on Information Assurance to government departments and, in certain circumstances, private companies. Further details (including recruitment information) are available at [www.cesg.gov.uk/about_us/careers.shtml](http://www.cesg.gov.uk/about_us/careers.shtml)
  - Security Service (MI5) - [www.mi5.gov.uk/careers/graduates.aspx](http://www.mi5.gov.uk/careers/graduates.aspx)
  - Secret Intelligence Service (MI6) - [www.sis.gov.uk/output/careers-1.html](http://www.sis.gov.uk/output/careers-1.html)

- **Law enforcement agencies**
  - The Information Assurance Advisory Council is a broad-based group concerned with minimising threats to the UK’s IT infrastructure. Its website lists its member organisations which include private companies, government agencies and academic research centres. - [www.iaac.org.uk](http://www.iaac.org.uk)
  - The Centre for the Protection of National Infrastructure (CPNI) is a government organisation, targeting primarily the critical national infrastructure (CNI) - those key elements of the national infrastructure which are crucial to the continued delivery of essential services to the UK. - [www.cpni.gov.uk](http://www.cpni.gov.uk).
  - The Communications Electronics Security Group (CESG) is the Information Assurance arm of the Government Communications Headquarters (GCHQ) and it provides advice on Information Assurance to government departments and, in certain circumstances, private companies. Further details (including recruitment information) - [www.cesg.gov.uk](http://www.cesg.gov.uk)
The Serious Organised Crime Agency (SOCA) is an intelligence-led agency with a remit and law enforcement powers to reduce the harm done to individuals and communities by serious organised crime. - www.soca.gov.uk/careers/opportunities

**Intelect** is the main trade association for the UK IT industry and it provides the secretariat for SAINT; the Security Alliance for Internet and New Technologies. - www.intellectuk.org

**The Serious Fraud Office** investigates major fraud of all kinds and it employs its own specialist IT staff. - www.sfo.gov.uk

- **IT software developers producing encryption software**
  - The *Computing MI IT Software* directory (available to the left of the green IT folders) lists software developers by software category, including ‘encryption’ under ‘security’.

- **Specialist consultancies in Information security**
  - The *Computing MI IT Services* directory (available to the left of the green IT folders) lists IT consultancies by specialisations, including ‘security’.

- **Professional services firms providing technology security services**

- **IT end-users where encrypted data is needed e.g. finance companies**

  - **Barclays** technology graduate programme - [www.barclays-graduates.co.uk/our-graduate-programmes/technology/about-technology](http://www.barclays-graduates.co.uk/our-graduate-programmes/technology/about-technology)

  - **Logica** technology graduate scheme - [www.logica-graduates.co.uk/our-programmes/pts-programme-and-technical-services](http://www.logica-graduates.co.uk/our-programmes/pts-programme-and-technical-services)


  - Vacancies with banks concerning security aspects of plastic cards, are few and far between and are often direct entry rather than featuring on any graduate training scheme.

- **IT management consultancies**

- **Telecommunications organisations**
  - **Siemens** security division - [www.siemens-enterprise.com/uk/services/security.aspx](http://www.siemens-enterprise.com/uk/services/security.aspx)

  - **RIM** (the company that operates BlackBerry) all their e-mail messages are encrypted. - [www.rim.com/careers/students/](http://www.rim.com/careers/students/)
• Broadcasting companies

The following is a job advertisement for a senior position in cryptology to indicate the kind of skills and knowledge that may be required for cryptology positions:

Security - Cryptography - Senior Consultant
Location: London, London, United Kingdom
Firm Service: Enterprise risk services
Type of Position: Full-time

Job Description
Our market leading Security, Privacy and Resilience practice has a proven track record of working on complex and high profile issues, with some of the UK’s leading organisations. We are uniquely positioned in being able to help our clients improve the security, privacy and resilience of a single component or to develop comprehensive security, privacy and resilience programmes.

Our fast growing practice is on the lookout for exceptional consultants in the field of cryptography.

Main purpose of job
To assist our clients in the design, delivery and ongoing operation of various cryptography capabilities such as Public Key Infrastructures (PKI), secure transmission of data (e.g., SSL/TLS, secure email), Hardware Security Modules (HSM) and centralised key management.

Specific cryptography responsibilities include:
- Defining project drivers and the underlying business case for cryptography–related solutions
- Analysis and definition of functional and technical requirements working with security and technology senior users
- Performing vendor assessments and technical proof of concepts to help our clients to select fit–for–purpose solution(s)
- Designing and deploying cryptography–related solutions
- Defining and embedding operations and support procedures to ensure effective handover of the cryptography–related solutions to client operational support teams
- Managing relationships with cryptography product vendors

Other responsibilities will include:
- Managing or co–managing delivery to provide exceptional service to the client, including defining a project's scope, approach, budget, plan and milestones, as well as managing project risks and issues
- Managing day–to–day client relationships and strengthening and broadening key client relationships
Identifying key client business issues and/or industry/market developments that help to define client needs

Determining client needs by supplementing the standard assessment techniques and tools with innovative approaches

Producing high–quality documentation in line with project deliverables (e.g., management reports, project briefs, business cases, operational procedures, etc.)

Reviewing deliverables of the team and verifying that they meet client and contract expectations

Participate in selling activities by applying learned techniques and approaches.

Taking an active role in supporting the achievement of business goals through practice initiatives

Generating innovative ideas that are strategically sound and progressive; challenging the status quo and fostering creativity on engagements

To be considered, you must possess:

- An excellent understanding of cryptography and related concepts and principles (e.g., encryption algorithms, hash functions, PKI, key exchange, certification authorities, digital signatures)
- An excellent understanding of cryptographic standards and protocols (e.g., PKCS, FIPS 140–2, IPSec, SSL/TLS)
- In–depth knowledge of at least two cryptography solutions from vendors such as PGP, Entrust, Cryptomathic, Ingrian, RSA, Voltage, Thales/nCipher and Blue Coat
- Experience of defining and establishing crypto key hierarchies and generation of master/root keys
- Strong academics, including a minimum of 2.1 degree or equivalent
- Understanding of information security principles and best practice (e.g., ISO27001, ISF Standards of Good Practice for Information Security)
- Man–management experience
- Excellent interpersonal skills
- Ability to think creatively to solve client needs
- A willingness to work across multiple clients in the private and public sector

Preferred:

- Hands–on experience in configuring and deploying HSMs
- Experience in coding to cryptographic APIs
- Qualifications such as CISSP, CCNA, CCNP, ITIL and PRINCE2